POLICY STATEMENT AND PURPOSE

This policy applies to Targa Resources Corp., including all of its subsidiaries and affiliates (collectively "Targa"). The purpose of this policy is to ensure the appropriate, responsible, and safe use of Targa Information,[1] Electronic Communication Systems,[2] and Electronic Communication Devices[3] (as referenced herein includes Personal Devices[4]) and to establish minimum standards for all Workers.[5] This policy is to be broadly interpreted to include new and improved technology not commercially available as of the issue date of this policy. Workers must also comply with other applicable Targa policies.

This policy sets standards for (i) the access and acceptable use of Targa's Electronic Communication Systems by its Workers, (ii) Workers' responsibilities as to the access, use, dissemination, publication, and disclosure of any Information sent, received, or obtained via electronic means or stored using Electronic Communication Systems, and (iii) Targa's rights of access to, responsibilities as to discovery of, and rights of recovery and deletion regarding Targa Information and the systems described hereunder. This policy also applies to all mobile and non-mobile Electronic Communication Devices that Targa owns and Personal Devices (as further described below) which have been used to access or otherwise interact with Targa Information. For example, this policy applies when a Worker uses a personal laptop, smart phone, or iPad to electronically access Targa's Information.

ELECTRONIC COMMUNICATION SYSTEMS AND RIGHTS OF TARGA

A Worker shall have no expectation of privacy regarding the Worker's activities on the Electronic Communication Systems, including the accessing of the Electronic Communication Systems through the use of any Personal Devices to the extent the Personal Device possesses Targa Information, whether on Targa premises or offsite. The Electronic Communication Systems and Targa Information that is composed, transmitted, or received via the Electronic Communication Systems are considered business records of Targa and the property of Targa. Consequently, personal or non-business matters and communications become Targa Information and business records if stored or transmitted via the Electronic Communication Systems. As such, Workers should not use the Electronic Communication Systems for matters intended to be private or personal. As an example, a Worker's use of a personal e-mail account to store or transmit Targa Information would result in Targa retaining the right to access such personal e-mail account so as to reclaim, produce, or delete any Targa Information accessible therein. As described in greater detail below in this policy, if a Personal Device is used to access, alter, store, or transmit Targa Information, Targa shall have the right to access such Personal Device so as to reclaim, produce, or delete any Targa Information accessible therein. Please note that a copy of any electronic record accessed from, or transmitted through, a personal messaging technology using the Electronic Communication Systems has the possibility of being stored in the Electronic Communication Systems. If such information is retained on the Electronic Communication Systems, Targa retains the right to review such records without consent and at its discretion. Targa may provide notice to any Worker whose Personal Device or personal records is to be accessed by Targa, although such notice need not be provided.

---

[1] "Information" means all raw or processed data and includes, but is not limited to, text, audio, image, and video files, word processing or other documents, presentations, models and spreadsheets that contain, document, or transmit raw or processed data that would independently be categorized as "Information."

[2] "Electronic Communication Systems" means any electronic, computer, or other digital system owned, provided, used, subsidized, or operated by Targa, including but not limited to, its computer network, technology system, phone system, voice mail, e-mail, computer-related equipment, software, files, disks, diskettes, flash or USB drives, DVDs, CD-ROMs, other removable media, or Electronic Communication Devices (including communications and messaging systems related thereto) that carries Targa Information.

[3] "Electronic Communication Device" means any device that can be used for: (a) word processing; (b) wireless Internet access; (c) image and sound capture or recording; or (d) transmittal, receipt, and storage of Information, including, but not limited to, e-mail, text messages, and other electronically-stored Information. Examples of these devices include, but are not limited to, laptops, tablet PCs, smart watches, iPads, cell phones, Blackberrys, and smart phones such as Androids or iPhones.

[4] "Personal Device" means any Electronic Communication Device privately owned by any Worker.

[5] "Worker" means any Targa director, officer, or employee, temporary or permanent worker engaged by Targa, authorized agent, third party, or independent contractor retained by Targa, and/or any volunteer providing services on behalf of Targa.

Targa retains the right to access, enter, search, inspect, monitor, and disclose any Targa Information, messaging communication (including e-mail, instant messages, mobile device text messages, and social media or other electronic messaging and collaboration and any archives thereof), records, and files on the Electronic Communication Systems, at any time and for any reason. Targa also retains the right to access, search for, inspect, and disclose any Targa Information contained on any diskette, flash drive, CD-ROM, DVD, or other removable media or on any Electronic Communication Device that is (i) linked to the Electronic Communication Systems, (ii) located on Targa property at its premises, or (iii) located with files or records that belong to or are provided by Targa, at any time and for any reason.

As a condition to permitting any Electronic Communication Device to access the Electronic Communication Systems, Targa retains the right to request that any Worker install an application (or "app") upon such Electronic Communication Device to aid Targa in the retrieval, production, or deletion of Targa Information from such device, regardless of where stored therein. Targa retains the right, by means of an app or otherwise, to retrieve, produce, or delete any Targa Information stored or that is otherwise accessible on any Electronic Communication Device that accesses or previously accessed the Electronic Communication Systems; however, Targa may only delete the entirety of any such device (including any non-Targa Information on the device) if (i) the applicable Electronic Communication Device is deemed lost or beyond the control of Targa and/or the Worker who owns such device, (ii) circumstances reasonably dictate (in Targa's sole discretion) that Targa Information will be compromised if such a blanket deletion does not occur, or (iii) upon termination of a Worker who does not request at the time of such termination to retain any non-Targa Information on the device. Pursuant to the foregoing, any Worker who uses a Personal Device to access the Electronic Communication Systems agrees to report immediately to the Information Technology ("IT") Department the loss or theft of a Personal Device on which such Worker has stored Targa Information or which is configured to access Targa Information or the Electronic Communication Systems.

The Electronic Communication Systems and any Personal Device using the Electronic Communication Systems should be used only to exchange Information that is business related subject to the limited exceptions herein. Under no circumstances may a Worker use any of the Electronic Communication Systems to send or receive illegal, harassing, offensive, obscene, hateful, or otherwise inappropriate messages or materials of any kind. Workers also are prohibited from using the Electronic Communication Systems, any Electronic Communication Device or any Personal Device while accessing the Electronic Communication Systems to solicit or engage in other activities on behalf of any outside business ventures, political campaign, charity, religious group, or similar engagements that are not part of the Worker's professional duties; excepting, however, minimal personal communication of an informal nature. Workers may use the Electronic Communication Systems for non-business reasons within the bounds of prudence and good judgment, but not in a manner that could compromise any Targa Information, harm productivity, embarrass Targa, or interfere with regular work duties of any Worker.

TERMINATION OF WORKER

Upon a Worker's termination of employment by or affiliation with Targa, such Worker has the following obligations and Targa retains the following rights:

- Worker must return all Targa Information and any Targa Electronic Communication Device (other than a Personal Device) in the Worker's possession;
- Targa retains the right to delete all Targa Information stored on any Personal Device and the right to access, retrieve, produce, or delete any Targa Information that may mistakenly or otherwise remain accessible on any Personal Device or personal e-mail of a former Worker;
- Worker submits to Targa's deletion of Targa Information on the Worker's Personal Device and acknowledges that such deletion may result in the Worker losing personal data stored on the Worker's Personal Device; and
- Targa retains the discretion to delete any non-business Information stored on the Electronic Communication Systems previously stored by the Worker (including documents, files, images, video, and music).

SECURITY ISSUES

At all times, Workers are responsible for maintaining the security of the Electronic Communication Systems and maintaining the integrity of all Targa Information. Workers are responsible for safeguarding Targa Information regardless of the location of that Information, including, but not limited to, Information on the Electronic Communication Systems, any Electronic Communication Device, any Personal Device, or on any other technology system. Even when authorized by this policy, Workers must not download or otherwise interact with any Targa Information on any Electronic Communication Device, including any Personal Device, unless the device is subject to the same or similar security protocols as those applicable to the Electronic Communication Systems.

Workers shall safeguard passwords and follow all Targa policies, procedures, and guidelines concerning services and systems security. Worker account or device passwords are not to be shared with others.

Regarding Targa Information or other business-related materials, Workers shall not, without the approval of IT, move, store, or otherwise relocate Targa Information in a manner that would move Targa Information onto any cloud computing services or programs, whether from a Targa-provided Electronic Communication Device or from a Personal Device. As used in this policy, "cloud computing services or programs" mean third-party services for accessing applications, storing data, or similar on-demand network access to non-Targa networks, such as YouSendIt, Dropbox, Snapfish, or GoogleDocs. Workers are prohibited from acquiring, possessing, or using any hardware or software tools that would compromise Targa Information. Whether through cloud computing services or programs, Personal Devices, or other non-Targa networks, Targa Information must not be stored in any manner in which the proprietary or confidential nature of the Information could be compromised.

Further, as part of Targa's security protocols, Workers with a Targa-issued Electronic Communication Device or a Personal Device with a camera feature shall not use that feature in any manner inconsistent with this policy.

INTERNET USAGE

Workers must adhere to Targa's Code of Conduct when accessing the internet through the Electronic Communication Systems.

Further, the Electronic Communication Systems have been equipped with virus-scanning and other security software. To the extent reasonably controlled by any Worker, anti-virus and other protective tools must be continuously enabled on Targa's Electronic Communication Systems and Electronic Communication Devices, including Personal Devices used to access Targa information. Further, Workers are prohibited from conducting any form of network or system monitoring beyond Targa's authorized monitoring protocol provided by the IT Department. Workers are prohibited from by passing Targa security controls.

Workers are provided access to the Internet via the Electronic Communication Systems to assist in performing tasks related to their jobs. The Internet can be a valuable source of information, but its use must be tempered with common sense and good judgment. Workers shall not "surf" the Internet on non-work related topics during work hours. Further, Workers shall not use the Internet to download movies, games, and/or other programs that are not related to their jobs. As previously stated, there should be no expectation of privacy as any search transaction using the Eectronic Communication Systems is the property of Targa. Targa reserves the right to monitor the usage of the Internet and block any site that may be deemed inappropriate, offensive, malicious, or represent a cybersecurity threat. Any inappropriate use of the Electronic Coummunication Systems, Targa Information or Electronic Communication Devices could result in disciplinary action up to termination.

MESSAGING USAGE

Messaging relates to the usage of all types of electronic communication technologies including but not limited to: 1) E-Mail 2) instant messaging 3) internal collaboration systems 4) mobile device text messages and any other form of communications provided by Targa ("Messenging Technologies"). Each of these technologies share a common theme in that communications are in electronically written form and may also include the sharing of file attachment(s) or URL links to one or many other Workers within Targa. In addition to the other restrictions of this policy, correspondence via messaging technologies should be prepared, received, and treated with the same care and formality as written, non-electronic correspondence. Messaging correspondence can and should be considered confidential and treated as described under Targa's Code of Conduct. Disclosure of confidential material could have adverse consequences to Targa's business. If a Worker is uncertain whether Information is confidential, the Worker should use caution and obtain approval from senior management or the Legal Department before transmitting such Information to persons outside of Targa. As previously mentioned, Workers should not assume or have an expectation of privacy while using Messaging Technologies. Targa reserves the right and ability to monitor and scrutinize any data within the Electronic Communications Systems.

While Messaging Technologies allow Workers to conduct business efficiently, usage comes with some inherent risks. Messaging records are legally discoverable and permissible as evidence in a court of law. Communications sent by the Messenging Technologies can never be unconditionally and unequivocally deleted. The possibility of discovery always exists. Workers should always use good judgement in determining if communication should be delivered electronically versus in person.

Workers should be mindful that these Messaging Technologies are a poor medium to convey mood and context – care, therefore, should be taken to consider how the recipient might interpret a message before composing and sending it. Workers should never use the Messaging Technologies to send disparaging, abusive, profane, or offensive comments or materials. More importantly, Workers should be vigilant to potential cyber attacks when using these Messaging Technologies. If any cyber threat is suspected immediately discontinue use and notifiy the IT Department.

Finally, Messaging Technologies are not considered the final system of record. Any formal Targa record needs to be properly stored in the appropriate system of record. As an example, a fully executed Contract between parties would be stored in

electronic form on a file share and not within an individual Worker's email. Workers may use Messaging Technologies to exchange records, but ultimately the information contained there must be properly stored in the appropriate system of record.

SOCIAL MEDIA AND SOCIAL NETWORKING USAGE

Activities on social networking or social media sites outside of work hours must comply with any applicable law, regulation, and any Targa policy if those activities relate in any way to or comment on Targa's business, employees, customers, or competitors. It is not appropriate to use Social Media for personal activities during work hours. Although Workers may reference their employment or affiliation with Targa generally in connection with personal social network accounts, they may not create social network accounts, postings, webpages, or blogs that appear to be affiliated with or endorsed by Targa or that violate any law, regulation, or Targa policy. Further, Workers are not authorized to speak on behalf of Targa or to represent that they do so in any social media websites without the express written approval by the executive management of Targa.

Should approval be given by Targa, Workers should always disclose their employment by or affiliation with Targa if their posting is an endorsement of Targa's products or services, i.e., expresses opinions, beliefs, findings, or experiences concerning Targa's products or services. Such content must have been reviewed or approved by Targa. Regardless of the above, Workers should never post any financial, confidential, sensitive, or proprietary information relating to Targa. Workers should be mindful that any comments made on Social Media could reflect poorly on the individual and/or Targa. To that end, when using Social Media be respectful of others and do not engage in discussions that may be offensive and damaging to the individual and/or Targa. Workers should understand that when making comments or sharing information on Social Media there is no anonymity – by definition these platforms are very public and once information is posted many people will have immediate access. Targa reserves the right to take appropriate action against Workers who missuse Social Media that negatively impacts Targa.

VIDEO CONFERENCING USAGE

Targa provides video conferencing services as part of the Electronic Communication Systems to connect Workers in a face to face manner. Video conferencing is intended for business purposes only. Communications which occur via video conferencing should adhere to the Code of Conduct Policy and be held to the same professional standards as in-person discussions and/or meetings. Video communications must not contain or have links that contain offensive, abusive or harassing language or content. Nor should they contain remarks that might be potentially embarrassing to Targa, its employees or the general public.

SOFTWARE

Targa provides certain software that it has selected for use with the Electronic Communication Systems. Workers are prohibited from installing unapproved or unauthorized software and executable files on the Electronic Communication Systems that present any threat or potential compromise of the Electronic Communication Systems. Further, all software must be purchased and accounted for through Targa's IT Department. Targa will not tolerate the illegal copying or distribution of software (for profit or otherwise). No Worker may engage in software piracy (copying, distributing, installing, or using software outside of the terms of the owner's license or without proper payment of any license fees). Software will be installed only by the IT Department, if Targa approves its use, the Worker has a legitimate license for such software, and such license is turned over to the IT Department for documentation.

COMPANY-OWNED ELECTRONIC COMMUNICATION DEVICES

Unless otherwise explicitly authorized by the IT Department, the IT Department is the sole procurer, supplier, service contract manager, and payment processor of company-owned Electronic Communication Devices. Specifically, P-Cards and T&E cards cannot be used to pay for company-owned Electronic Communication Devices and the associated monthly fees. Vice Presidents (or Department Heads specifically designated by a Vice President) and Area Managers shall determine which Workers within their departments qualify for a company-owned Electronic Communication Device and can order a device through the IT Service Desk. Models and brands of company-owned Electronic Communication Devices are solely determined by the IT Department and the IT Department will support, troubleshoot, upgrade, replace, and service any company-owned Electronic Communication Devices. Such requests should be made through the IT Service Desk.

PERSONAL DEVICES

If authorized by the IT Department, a Worker is allowed to use a Personal Device or other public, shared device to access Targa's Electronic Communication Systems and Targa Information; provided that any such access or storage of Targa Information on a Personal Device complies with all of Targa's applicable policies. Such requests for access should be made through the IT Service Desk. Before using any Personal Device, Workers must confirm with the IT Department that the Personal Device has adequate security protocols in use. If requested by the IT Department, the Worker will allow the IT Department to install a Mobile Device Management ("MDM") client on the device. The MDM client can be used to install, protect, manage, and maintain Information

and software that is installed on the Personal Device. Failure to allow and maintain the installation of the MDM client on the Personal Device will terminate the Worker's access on that device.

If interfacing with the Electronic Communication Systems on a Personal Device, a Worker may not use the Personal Device in a manner that could compromise Targa Information, harm productivity, embarrass Targa, or interfere with regular work duties of any Worker.

Notwithstanding the other provisions of this policy, a Personal Device is considered part of the Electronic Communication Systems; however, it is only considered as such to the extent it contains any Targa Information. If a Worker accesses, alters, or stores Targa Information on a Personal Device, Targa retains rights of recovery, deletion, and discovery as to the Personal Device so that Targa may recover, delete, or discover Targa Information transmitted or altered on such device. Please note that other Information that is not Targa Information on a Personal Device or other device that is not owned or operated by Targa is (i) subject to reasonable expectations of privacy and independent ownership, (ii) not considered the property of Targa or the business records of Targa and not discoverable or required to be produced by Targa, and (iii) other than what may be affected by the deletion rights enumerated under this policy, not otherwise to be controlled by Targa.

Each Worker procures and maintains sole ownership of any Personal Device. Any costs incurred in connection with the initial purchase, replacement, ongoing maintenance, or upgrade of a Personal Device is the responsibility of the Worker and will not be reimbursed by Targa. Targa is not financially responsible for lost, stolen, or broken Personal Devices, even if such event occurs while conducting Targa business.

Under no circumstance will the IT Department support, upgrade, troubleshoot, replace, or service a Personal Device; the Worker has the sole responsibility to seek help from the Personal Device service provider. The IT Department will only assist employee with configuring the Personal Device with the following services:

- Installation of Targa MDM client software
- Synchronization and setup of Targa corporate email
- Assistance with any Targa mobile applications

RIGHTS OF ACCESS

Targa has the right to access any physical workplace area at any time on its premises, including a Worker's office, cubicle, desk, file cabinets, lockers, closets, or the like. If such areas or items are required to be locked away for business purposes, keys or combinations to any locks shall be made available upon the request to the proper Targa personnel conducting the search. All Workers are subject to Targa's foregoing right to access and search; Workers do not have an expectation of privacy with respect to such areas being accessed and searched. All Workers are subject to Targa's rights to access, enter, search, inspect, and disclose as discussed above in this policy.

VIOLATIONS AND PENALTIES

Any violation of this policy must be immediately reported to Targa's Human Resources department, IT Department, and/or the office of the CIO.

Violation of this policy or any of its rules, guidelines, or tenets may result in disciplinary action, up to and including, termination of employment or affiliation with Targa, or termination of the contract or assignment for contractors, and possible civil and criminal prosecution under local, state, and federal laws and regulations.

Targa reserves the right to change or deviate from its published policies, practices, and procedures at any time without prior notice as circumstances or business needs dictate.