

CORPORATE INFORMATION SECURITY

I. PURPOSE

The purpose of this policy is to set forth the corporate requirements for information security.

II. SCOPE

This policy applies to all Citizens Energy Group (Citizens) workforce members, including employees, Contingent Workers, partners, collaborators and any others doing business with Citizens involving Citizens' computers, technology systems, and/or data.

III. DEFINITIONS

Contingent Workers - Independent contractors, consultants, vendors, or other outsourced and non-permanent workers.

Information Security Incident – An event that compromises, or has the potential to compromise, the integrity, confidentiality, or the availability of Citizens systems and data.

IV. CHARTER

1. Citizens shall deploy a security management function capable of effectively minimizing the risk associated with the confidentiality, integrity, and availability of corporate data and information.
2. This function is responsible for implementing controls throughout the organization necessary for minimizing information security risk.
3. Key drivers of information security controls design are risk minimization, legal and regulatory compliance requirements, and system performance.

V. POLICY

1. Management of the Information Security Program
 - a. The VP of IT is the officer with primary accountability for the Information Security Program. The Director of Information Security maintains responsibility for execution of Citizens Information Security Program.
 - b. The VP of IT and Director of Information Security meet with the Board of Directors and provide updates on the status of Citizens Information Security Program.
 - c. The IT Department shall maintain evidence of direction provided for security from the Board of Directors, Executive Management, and other members of Management as directed. Evidence shall be maintained in the IT Process Asset Library (PAL) on the corporate intranet site (currently iTrust).
2. Information Security Plan

- a. IT shall maintain an Information Security Plan updated annually with the following components:
 - I. Top Information Security Risks with Mitigation Strategies
 - II. Security Awareness Training Requirements
 - III. Projected Investments in Security Processes
- b. The Information Security Plan shall use as inputs the Citizens Strategic Plan, IT Strategic Plan, the IT Departmental Risk Register and the Enterprise Risk Management process.
- c. Information security requirements shall be incorporated into Citizens processes via the IT Architectural Review of IT projects, the SCADA Working Committee, and the IT Service Level Expectations and Operating Level Expectations meetings with the organization.
- d. IT personnel shall adhere to an *IT Departmental Information Security Policy* which expands on and supplements the Corporate Information Security Policy.
- e. IT shall conduct stakeholder communications as follows:

What	Who	When	How
Changes to Information Security Policies and Procedures	Citizens Employees	At time of approval	Per the standard policy and procedure change management process
Information Security Plan and Strategies	Executive Management	Annually	Per the IT Strategic Plan reporting process

3. Information Security Standards and Data Classification Standard

- a. IT shall maintain the *Corporate Information Security Standards and IT Information Security Standards*.
- b. All Citizens workforce members, as defined in Section II Scope, shall adhere to the standards and guidelines set forth in the *Corporate Information Security Standards* included in Appendix A and the *Acceptable Use Policy*.
- c. Citizens workforce members must immediately report an actual or suspected security incident that involves unauthorized access to electronic systems owned or operated by Citizens; malicious alteration or destruction of data, information, or communications; unauthorized interception or monitoring of communications; and any deliberate and unauthorized destruction or damage of IT resources to the IT Support Center or directly to IT Information Security.
- d. IT shall maintain a *Data Classification Standard*. See Appendix B.

VI. PROCEDURE

Refer to Appendices A and B.

Primary Business Unit Owner: Vice President of Information Technology

Revision Date: September 19, 2025

Next Review Date/Year: 2028

Supersedes: Policy Release # 2016, Februaury 16, 2021

Reference: Acceptable Use Policy (Policy Release 2021)

"Citizens Energy Group at its option reserves the right to change, delete, suspend, or discontinue parts of the policy in its entirety, at any time without prior notice."

APPENDIX A CORPORATE INFORMATION SECURITY STANDARDS

I. PURPOSE

The purpose of this document is to provide a set of information security standards that ensure the confidentiality, integrity, and availability of the information assets owned or operated by Citizens workforce members.

II. SCOPE

These standards apply to all Citizens information assets, including, but not limited to computers and computer related hardware, software, data, printouts, mobile devices (including cellular phones, tablets or smartphones), printers, copiers, plotters, applications, USB drives, email and file transfers, telephone equipment, and any other information assets used in the course of business by Citizens workforce members.

III. DEFINITIONS

Administrative Account – Administrative accounts, service accounts, database administrative accounts are all unique to the Information Technology (IT) Department. These accounts are governed by the *IT Departmental Information Security Policy* and related standards.

Data Owner – The individual(s) who is accountable for the quality of a defined dataset.

Least Privilege – The concept that user access to data is limited to only that data required for performing the user's job responsibilities.

Mobile devices - Smart phones or tablets. (Laptops are subject to computer standards.)

Standard Account - An authentication account used by a Citizens workforce member for network access or application access for normal daily activity. Standard accounts are unique to each workforce member.

IV. STANDARDS

Section	Standard	Additional
Application/System Access	Authentication and Authorization	1. Access to Citizens information systems and data shall be authorized only by the Data Owner.

Section	Standard	Additional
		2. All workforce members shall be authenticated at each logon before accessing Citizens information systems and data.
	Provisioning, Deprovisioning and Modifying Access	<p>1. Access to any application or system shall be provisioned on the principle of 'Least Privilege'. Users shall be granted the minimum access required for their role and job responsibilities.</p> <p>2. Every employee with direct reports shall document job transfers and terminations in the Human Resources Information System (HRIS) immediately. Note: If unsure, user access can be temporarily terminated and reestablished at a later date.</p> <p>3. Access to Citizens information systems and data shall be disabled within 24 hours of receiving notification of the workforce member's departure.</p> <p>4. Access to Citizens information systems and data shall be modified as requested by Citizens Management within 24 hours of receiving notification of a job transfer.</p>
	Vendor Access	Vendor access to Citizens information systems and data for the purposes of system maintenance and upgrade activities shall be monitored and access shall be limited to only the specified working time frame.
	Contingent Worker Access	Contingent worker access must be sponsored by a Citizens employee and must be limited to the terms of the contract or 30 days, whichever is less. If extended access is needed, the Citizens sponsor responsible for the Contingent Worker must submit a request to renew the access. Access

Section	Standard	Additional
		can be extended for periods of up to 30 days at a time.
	Local Administrative Access	Local administrative access shall require the approval of the workforce member's manager and the IT Security Department and shall only be approved for valid business reasons.
	Privileged User Terminations	Access terminations for privileged users (e.g., Administrators) must be performed in an expedited manner. The workforce member's manager or supervisor must notify the Manager of Security and Compliance or the IT Security Engineer as soon as they are aware that the privileged user is no longer part of the workforce or is transferring to a position that does not require privileged access. Upon notification, the IT Security Department shall confirm that the privileged access is terminated immediately.
Authentication	Default and vendor-provided Memorized Secrets (passwords or PIN's) <i>Passwords are alphanumeric secrets.</i> <i>PIN's are numeric secrets.</i>	Default and vendor-provided Memorized Secrets shall be changed prior to the system being utilized for production or Citizens data being hosted by the system or application.
	Memorized Secret storage	Citizens account Memorized Secrets shall not be stored in any of the following unsecure manners, methods, or locations: <ol style="list-style-type: none"> <li data-bbox="1090 1558 1400 1670">1. Unencrypted digital file format (e.g. plain text document, csv file, etc). <li data-bbox="1090 1670 1400 1854">2. Unsecure physical location (e.g. openly visible locations such as a desk area post-it notes, physical notebook pages, etc). <li data-bbox="1090 1854 1400 1911">3. Unsecure digital locations (e.g. non

Section	Standard	Additional
		<p>corporate managed software solutions such as password managers, non corporate managed mobile devices, non corporate managed computers, or any other non corporate managed digital/physical devices without proper prior authorization).</p> <p>Where necessary, the IT Department can assist with identifying an appropriate Memorized Secret management mechanism.</p>
	<p>Memorized Secrets shall not be shared with others.</p>	<ol style="list-style-type: none"> 1. Do not share Memorized Secrets with anyone, including co-workers, family members, friends, vendors, etc. 2. Do not ask anyone for a Memorized Secret. 3. Do not talk about a Memorized Secret to anyone. 4. Do not reveal a Memorized Secret on questionnaires, forms, or documents of any kind.
	<p>Unique Memorized Secrets</p>	<p>Memorized Secrets must be unique when they are created and must remain unique throughout their lifecycle.</p>
	<p>Password length & complexity requirements.</p> <p>Password use cases:</p> <ul style="list-style-type: none"> - Network Access - Active Directory accounts - Linux accounts - Applications that host, process, or otherwise have access to Citizens organization data. 	<ol style="list-style-type: none"> 1. Passwords must be at least eight (8) characters in length and include at least three of the following: <ul style="list-style-type: none"> • Capital (upper case letters) • Lower case letters • Numbers • Special characters 2. Passwords must not be based on the user's name or login ID. 3. Do not use social security number or employee identification as a password.

Section	Standard	Additional
	Password Aging	<p>Passwords for Standard Accounts must be changed every 90 days when using up to 11 characters.</p> <p>Passwords for Standard Accounts must be changed every 12 months when using 12 or more characters</p>
	Password History	At least 1 year passes before a password may be recycled.
	Initial and Temporary Memorized Secrets	Initial Memorized Secrets or temporary Memorized Secrets issued from credential resets must be changed upon first login.
	<p>PIN length & complexity requirements.</p> <p>PIN approved use cases:</p> <ul style="list-style-type: none"> - Local Client Device Access <p>**PIN entries may not be utilized for authentication unless otherwise approved within this policy document.</p>	<ol style="list-style-type: none"> 1. PIN's must be at least six (6) numeric characters in length. 2. PIN's should not repeat the same numeric value more than twice consecutively. For example, the following PIN entries are not acceptable "111111" and "999555". 3. PIN's should not exist in chronological or reverse chronological order. For example, "123456" and "987654" are not valid PIN entries.
	<p>Biometric requirements.</p> <p>Biometric approved use cases:</p> <ul style="list-style-type: none"> - Local Client Device Access <p>**Biometric data may not be utilized for authentication unless otherwise approved within this policy document.</p>	<p>Biometric examples:</p> <ol style="list-style-type: none"> 1. Fingerprint scan 2. Face scan
	Lockout	<p>Standard accounts – account lockout for 30 minutes after 5 failed logins.</p> <p>Mobile devices– After 10 failed login attempts, device must locked requiring</p>

Section	Standard	Additional
		administrative unlock or wipe corporate data .
	Responsibility and Reporting	<p>Users are responsible for protecting the confidentiality of their Memorized Secrets and securing them against unauthorized disclosure.</p> <p>Users must immediately report any compromise or suspicion of compromise of their standard or mobile account Memorized Secrets to IT Security or the Support Center.</p>
	<p>Compromised authentication secrets</p> <p>Including, but not limited to:</p> <ol style="list-style-type: none"> 1. Memorized Secrets 2. Hardware/Software keys 3. OTP's 4. Tokens 	<p>Any authentication secret that has been compromised shall be reported to the Support Center. The Support Center shall determine the correct method for revoking the key or changing the password, minimizing potential loss and notifying stakeholders.</p>
	Untrusted devices	<p>Untrusted devices require MFA to access Citizens organization data or network.</p> <p>An example of a “untrusted device” is a personally-owned device which is not administered by Citizens.</p>
	Multifactor Authentication (MFA) requirements	<p>All MFA is required to meet the minimum specifications of NIST 800-63b-4.2pd Authentication Assurance Level 2 or AAL2.</p>
User ID's	Sharing	<p>Shared standard or mobile device accounts are prohibited without a documented exception. Users shall not provide anyone their user credentials (user id plus password) Passwords shall immediately be changed upon completion of the work requiring the shared credentials.</p> <p>Note: Limited-access system kiosks and meeting room computers installed with a special local account used for</p>

Section	Standard	Additional
		presentations may require the use of a shared User ID.
Citizens Networks	Personal and vendor equipment	Personal or vendor equipment should not be used on Citizens Corporate Business network. (This excludes the Citizens Employee Wireless Network and the Citizens Guest Wireless Network) without the approval of Citizens IT Security. Personal and vendor equipment may be used to access isolated applications hosted in Citrix.
	Remote access	The approved method of remotely accessing Citizens' networks from personally owned devices is via Citrix. VPN is used to allow remote access for Citizens owned and managed devices.
Equipment	Physical security of laptops and mobile devices	Users assume responsibility to reasonably secure Citizens-provided laptops and mobile devices when taken offsite.
	Loss or damaged equipment	Users must immediately report lost company equipment to the IT Support Center. Damaged equipment must be returned to the IT Support Center for proper disposal of equipment and resident data.
Software	Unauthorized software	Only approved software shall be installed on Citizens devices. Pirated or copyright-infringed software must not be installed and used on Citizens-owned devices for any business reason.

APPENDIX B DATA CLASSIFICATION STANDARD

The following table represents data generated or used by Citizens Energy Group considered to be Public, Internal, Sensitive or Restricted in nature. This list is not intended to be complete, but representative. Combinations of data considered Internal or Public may also be considered sensitive or restricted. The Data Owner retains the responsibility for classifying data that doesn't fit the examples below. Proper handling of data based on classification is also detailed in this section.

Public	Internal	Sensitive	Restricted
Risk Level:			
No Risk Low Value	Low Risk Low/Medium Value	Moderate Risk Medium/High Value	High Risk High/Critical Value
Definition:			
Information that can be disclosed to anyone. Does not violate privacy. Knowledge of this information will not expose the organization to financial loss, loss of business, loss of integrity or loss of an asset.	Information that relates to the operation of the business. This information is limited to access within Citizens Energy Group and to appropriate business partners.	Unauthorized disclosure, destruction, or compromise would have an adverse impact on the organization, our customers, or employees. Financial loss, damage to our reputation and integrity, loss of business and potential legal action may occur. Information is limited for use solely within the organization on a need to know basis.	Unauthorized disclosure, destruction, or compromise would result in substantive loss or severe damage to Citizen's integrity, severe financial liability, and significant advantage to a competitor, financial penalties, or serious violation of regulatory and legal requirements. Information is intended for internal organization use only on a strict need to know basis.
Access and Storage:			
Minimum control. If copyrighted, it may require read only and control over the ability to modify the content.	Access controls will limit access to the organization personnel and appropriate business partners. Control may focus on limiting the ability to modify the information. Modification of content may require prior approval. Control over this information is a business unit option.	Access is granted upon documented request and approval and based on appropriate need to know. Access is controlled by an ID and password. Directories and files are properly secured. Distribution is controlled. Audit trails will track information modification where deemed appropriate by Information Technology Management.	Requires formal documented request and approval based on an explicit predetermined need to know. Granting access requires strict and explicit accountability for the security of the information. Access is controlled by an ID and password and may require additional authentication. Directories and files are secured with limited user access. Audit trails track information modification

Public	Internal	Sensitive	Restricted
Risk Level:			
<i>No Risk Low Value</i>	<i>Low Risk Low/Medium Value</i>	<i>Moderate Risk Medium/High Value</i>	<i>High Risk High/Critical Value</i>
Storage Media:			
Minimum control. If copyrighted, it may require read only access and control over the ability to modify the content.	Storage and retention is managed by the individual business unit.	Storage and retention requires appropriate security and may require data encryption. Storage on mobile storage devices are approved by the Information Owner and are fully supported by business justification.	Storage and retention requires appropriate security and may require data encryption. Storage on mobile storage devices are permitted based on a policy exception basis and are approved by the Information Owner and Information Security with appropriate security controls defined and implemented.
File Transmissions and Encryption:			
May occur over public network.	Does not require encryption. Transmissions to external sources are limited on a need to know basis.	Data is encrypted when transmitted outside the organization. Recipients and senders verify that only authorized persons will have access. Disclosure outside of the organization requires approval by the Information Owner. External disclosure requires a non-disclosure agreement.	Data is encrypted when transmitted outside the organization. Disclosure is based on a documented need to know basis. Recipients and senders verify that only authorized persons have access. Disclosure outside of the organization requires approval by the Information Owner. External disclosure requires a non-disclosure agreement.
External E-mail:			
Use standard e-mail confidentiality message.	Use standard e-mail confidentiality message. Require receipt/confirmation of receipt by intended recipient.	Use standard e-mail confidentiality message. Encrypted and secured with verification of receipt by the intended recipient.	Use standard e-mail confidentiality message. Encrypted and secured with verification of receipt by the intended recipient.
Mailing and Shipping Electronic Storage Media:			
Use transmittal with standard confidentiality message.	Use transmittal with standard confidentiality message. Require receipt/confirmation of receipt by intended recipient.	Use transmittal format with standard confidentiality message. Data is encrypted when sent to external destinations. Verification that materials sent have been received	Use transmittal form with standard confidentiality message. Data is encrypted when sent to external destinations. Verification that materials sent have been received

Public	Internal	Sensitive	Restricted
Risk Level:			
<i>No Risk Low Value</i>	<i>Low Risk Low/Medium Value</i>	<i>Moderate Risk Medium/High Value</i>	<i>High Risk High/Critical Value</i>
		by the intended recipient is required. Proof of receipt/audit trails may include a signed receipt, e-mail or other returned document or token verifying receipt.	by the intended recipient is required. Proof of receipt/audit trails may include a signed receipt, e-mail or other returned document or token verifying receipt.
Facsimile Transmissions:			
Use fax cover sheet with standard confidentiality message.	Use fax cover sheet with standard confidentiality message.	Use fax cover sheet with standard confidentiality message. Request confirmation of receipt.	Use fax cover sheet with standard confidentiality message. Establish a transmission schedule and receipt verification process with the intended recipient that ensures only the recipient receives the document.
Copying:			
May be copied and printed in public area.	May be copied as required. Distribution is limited to those with a need to know.	Copying is limited and restricted to Internal use only unless a specific policy exception has been submitted and approved by the business unit manager.	Copying is restricted and limited to internal distribution unless specifically authorized otherwise approved by a Citizens Officer.
Posting of Intranet Content:			
May be displayed in an unsecured mode.	May be displayed in an unsecured mode.	Display in a secured environment that limits access to those who need it to fulfill job responsibilities.	Display in a secured environment that limits access to those who need it to fulfill job responsibilities.
Workplace Communication/Sharing Information:			
This information may be widely shared among employees and appropriate external people.	This information is shared with employees and other groups on a need to know basis and for the purpose of supporting the efficient operation of the organization.	This information sharing is limited to individuals who require the information to properly service the customer. The sharing of the information verbally or in documented form is performed with discretion and with the awareness of the commitment to customer confidentiality.	This information sharing is restricted to those individuals who have a need to know. The sharing of information verbally or in documented form is confidential and secured and is performed with discretion and with the awareness of Citizen Gas commitment to customer confidentiality. This information is never publicly discussed or disclosed.
Disposal of Electronic Media:			
No security requirements.	Electronic media is erased on all PCs prior to redeployment; expiration dates are assigned to all electronic media and to all documents (paper and	Media is discarded in containers provided for destruction or shredded internally; electronic media is erased on all PCs prior to redeployment; expiration	Media is discarded in containers provided for destruction or shredded internally; electronic media is erased on all PCs prior to redeployment; expiration

Public	Internal	Sensitive	Restricted
Risk Level:			
<i>No Risk Low Value</i>	<i>Low Risk Low/Medium Value</i>	<i>Moderate Risk Medium/High Value</i>	<i>High Risk High/Critical Value</i>
	electronic) by the Business Unit in accordance with Citizens Energy Group Records Retention Schedule, and the media is erased upon expiration; spreadsheets, Word documents and Access databases are deleted when no longer required.	dates are assigned to all electronic media and to all documents (paper and electronic) by the Business Unit in accordance with Citizens Energy Group Records Retention Schedule and the media are erased upon expiration; spreadsheets, Word documents and Access databases are deleted when no longer required.	dates are assigned to all electronic media and to all documents (paper and electronic) by the Business Unit in accordance with Citizens Energy Group Records Retention Schedule and the media is erased or destroyed upon expiration; spreadsheets, Word documents and Access databases are deleted when no longer required.