# INFORMATION SECURITY PROGRAM POLICY

**Responsible Official:** Chief Information Security Officer

**Effective Date:** 05/1/2019
**Last Review Date:** 05/1/2019

## Objective

This document provides definitive information on the prescribed measures used to establish and enforce the Information Security Program at UGI Corporation and its subsidiaries and affiliates (collectively, "UGI").

## Purpose

UGI is committed to protecting its employees, partners and clients from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every UGI user who interacts with data and information systems.

Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- Integrity – addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and information systems. This also includes against accidental loss or destruction.

The purpose of UGI's Information Security Program is to:

- Protect the confidentiality, integrity, and availability of UGI data and information systems.
- Protect UGI, its employees, and its clients from illicit use of UGI information systems and data.

- Ensure the effectiveness of security controls over data and information systems that support UGI operations.

- Recognize the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related Information Security risks.

- Provide for development, review, and maintenance of minimum security controls required to protect UGI data and information systems.

Implementing consistent security controls across the company will help UGI comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity, and availability of UGI data.

## Scope

This policy applies to all employees, contractors, temporary workers and affiliates handling and/or processing UGI information.

## Policy

In an effort to ensure an acceptable level of Information Security risk, UGI has developed a coherent set of policies, standards and guidelines to manage risks to its data and information systems.

UGI users are required to protect and ensure the Confidentiality, Integrity, and Availability (CIA) of data and information systems, regardless of how its data is created, distributed or stored. Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and information system. Security controls must be designed and maintained to ensure compliance with all legal requirements.

## Key Terminology

In the realm of Information Security terminology, the National Institute of Standards and Technology (NIST) IR 7298, Revision 2, Glossary of Key Information Security Terms, is the primary reference document that UGI uses to define common security terms. Key terminology to be aware of includes:

Asset Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, to assure that the assets are used for the purposes intended, and assure that information regarding the equipment is properly documented.

Cardholder Data Environment (CDE): A term describing the area of the network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment

Control: A term describing any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help UGI accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Control Applicability: A term describing the scope in which a control or standard is relevant and applicable.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align UGI with accepted due care requirements.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies. The Data Classification & Handling Guidelines provides guidance on data classification and handling restrictions.

Data Owner: A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense. Asset owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained, and used.

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Information Security: A term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, and Availability (CIA) of data.

Information System: A term describing an asset; a system or network that can be defined, scoped, and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

Procedure: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.

Sensitive Data: A term that covers categories of data that must be kept secure. Examples of sensitive data include Personally Identifiable Information, Electronic Protected Health Information (ePHI), and all other forms of data classified as Restricted or Confidential in the Data Classification & Handling Guidelines.

Personally Identifiable Information (PII): PII is commonly defined as the first name or first initial and last name, in combination with any one or more of the following data elements:

- Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
- Driver License (DL) or another government-issued identification number (e.g., passport, permanent resident card, etc.)
- Financial account number
- Payment card number (e.g., credit or debit card)

Standard: A term describing formally established requirements in regard to processes, actions, and configurations.

Target Audience: A term describing the intended group for which a control or standard is directed.

## Violations

Any UGI user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law will be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

## Exceptions

While every exception to a policy or standard potentially weakens protection mechanisms for UGI information systems and underlying data, occasionally exceptions will exist. Procedures for requesting an exception to a policy or standard are available in the 'UGI Policy Exception and Risk Assumption Process' document.

## Ownership and Maintenance

This Policy is scheduled for review and revision on an annual basis or at such other times as deemed appropriate or necessary. The Chief Information Security Officer is responsible for ensuring this Policy's appropriateness through reviews and revisions, with support from the Legal, Compliance and Internal Audit departments.

## Revision History

| Rev. Date | Revised by | Reason for Revision |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |