GATHERACT LLC.

INFORMATION SECURITY MANAGEMENT PROGRAM

Date of version:	01-June-2021
Version number:	1.0
Approved by:	Joe Crop - CEO

Change history

Date	Version	Created by	Description of change
07-May-2021	0.1	Carlos Vinícius Costa - CTO	Initial draft
01-June-2021	1.0	Joe Crop - CEO	Final version

Table of contents

1. Purpose

This program document establishes the information security, privacy, and compliance program's requirements and responsibilities to establish the information security, privacy protection, and compliance framework for GatherAct LLC. (hereafter the "Company").

2. Scope

This program applies to all company information processing systems and facilities, including those managed for the company's customers. This policy applies to all employees, partners, and third parties to access the company's information assets.

3. Reference documents

- ISO/IEC 27001:2013 Clause 5, 6 and 7

4. Definitions

Information system – includes all servers and clients, network infrastructure, system, application software, data, and other computer subsystems and components owned or used by the organization or under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.

Information assets – In this Policy's context, the term *information assets* is applied to information systems and other information/equipment, including paper documents, cloud-based service, virtual storage, and backup solutions.

Information security – The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Information security risk – The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems.

PDCA – The Plan, Do, Check, Act method is used to provide a continuous improvement framework for procedures.

Policy - Statements, rules, or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component.

5. Information Security Management (ISO 27001 C.5.1, C.5.2, C.5.3)

5.1. Background

GatherAct management decided to create a long-term information security management program to improve the existing security framework and formally assess and improve its security maturity. GatherAct long-term vision is to provide appropriate third-party assurance and compliance reports by the ISO/IEC 27001:2013 framework.

5.2. 5.2. Management Program Policy (ISO 27001 A.18.1.1, A.18.1.4)

Information Security Program: The company will implement a comprehensive, written information security program that secures its information assets in a manner commensurate with each asset's value as established by risk assessment and mitigation measures.

Information Privacy Program: The company will implement a comprehensive, written information privacy program that secures its employee and customer personally identifiable information (Pll} against unauthorized use or disclosure.

Compliance Program: The company will collect all legal, regulatory, and contractual requirements and implement a compliance management program to ensure the identified requirements are fulfilled.

5.3. Program goals

The company will implement an Information Security Management System based on the ISO/IEC 27001/02 standards' requirements and controls.

Information Security Policies: Policies must be implemented and enforced to assure the security, reliability, integrity, and availability of the company's information assets. The information security program must contain policies and procedures that define:

- Information asset identification and classification
- The risk assessment process
- The enterprise-wide technical and administrative security controls
- Software Development Life Cycle
- Security testing
- Third-party provider and vendor risk and delivery management
- Appropriate requirements for the periodic review and updates of the information security management program
- Appropriate requirements for reporting to GatherAct management
- The safeguarding of customer information
- Business Continuity and Disaster Recovery planning
- Incident detection and response

Information Security Procedures: The CTO is responsible for creating, implementing, and enforcing security procedures and assuring the security, reliability, integrity, and availability of the company's information assets. The required controls must be identified along with the risk assessment. They shall be proportional to the identified level of risks and to be able to fill the identified compliance requirements.

Incident management: Policies and procedures will be implemented and enforced to protect the company's information assets against accidental or unauthorized modification, disclosure, or destruction (please see the Incident Response Plan).

Compliance management: Procedures must be implemented to ensure that the company can capture regulatory, contractual, and obligatory requirements (please see the Governance, Risk, and Compliance management policy).

Resources: The company will dedicate the appropriate resources to ensure the implemented security controls and framework's efficient operation.

5.4. Program management

Information security is a management responsibility, and the decision-making for information security must not be delegated. While specialists and advisors play an essential role in ensuring that controls are appropriately designed, functioning correctly, and adhered to consistently, the management is primarily responsible for information security.

The company's CEO is overwatching the information security management program; the CTO actively manages and delivers the program's elements. The management team meeting is held every month, where information security is actively discussed within the senior management team. The CTO is supported by the broader technical and development team.

5.4.1. Program Agenda

The company aims to achieve independent third-party certifications by the ISO/IEC 27001:2013 standard at the end of Q2 2022.

5.4.2. Responsibility Assignment (ISO 27001 C.5.3)

Information Security Officer: The CTO is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures.

Information Security Management Team: The information security management team composed of senior managers or their delegates meets every month to review the status of information security at GatherAct, to approve and later review information security projects, approve new or modified information security policies and perform other necessary high-level information security management activities.

Information Security Resources: Management must allocate sufficient resources and staff attention to address information systems security adequately. The CTO is supported by the company's technical team.

Clear Assignment of Control Accountability: The company's management must assign and document accountability for its internal control. This accountability must include sufficient transparency to keep top management informed about these same internal controls' effectiveness and efficiency.

Information Ownership Assignment: The senior management team must specify in writing the assignment of Information Ownership responsibilities for those product systems, databases, master files, and other shared collections of information used to support production business activities.

5.4.3. RACI Matrix

	CEO	**CTO**	**Senior leadership**	**Technical team**
Information Security Policies and procedures	A	R	I	C
Incident management	A	R	I	R
Resources	A	C	I	I
ISO 27001:2013 compliance	A	R	C	R
KPI's and IS program mgmt.	A	R	I	R

R = Responsible, A = Accountable, C = Consulted, I = Informed

5.4.4. Information Security Roles and Responsibilities (ISO 27001 C.5.3)

To coordinate a team effort, the company has established three categories, at least one of which applies to each employee and subcontractor. These categories are Owner, Custodian, and User. These categories define general responsibilities concerning information security.

Owner Responsibilities: Information Owners are the managers, members of the top management team, or their delegates who bear responsibility for the acquisition, development, and maintenance of production applications that process the company's information. The information owners are also responsible for protecting the knowledge collected, held, and created within the organization regardless of the information written electronically or verbally.

Production applications are computer programs that regularly provide reports in support of decision-making and other business activities. All production application system information must have a designated Owner and all information stored and managed within the corporate environment.

For each type of information, Owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users are granted access, and approve requests for various ways in which the information is utilized.

Custodian Responsibilities: Custodians are in physical or logical possession of either the company's information or information that has been entrusted. While technical staff members and developers are Custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the User is also a Custodian. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure and making backups so that critical information is not lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

User Responsibilities: Users are responsible for familiarizing themselves with and complying with all Divio policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to the Custodian or the information owner.

5.4.5. Information Security Management Program Reporting (ISO 27001 C.9.3)

The CTO is responsible for identifying the KPIs and reporting for the Information Security Management Program. Quarterly reports presented to the company's senior management that includes information on:

- The status of the program
- The updated risk assessment and analysis
- Management decisions for the level of risk mitigation and residual risk accepted.
- Service provider oversight activities and status
- The results of testing of essential controls
- Management's response to any identified deficiencies and recommendations for program changes
- The independent validation of the information contained in the report

5.5. Program Review and Maintenance (ISO 27001 A.18.2.1)

The information security program must be updated and reapproved by the company's management annually or on a material change in the organization or infrastructure. The information security program must be updated, as appropriate, based on the organization's risk assessment results and any risk assessment completed by third parties.

An independent and externally-provided review of information systems security must be periodically obtained to determine both the adequacy of and the compliance with controls. The appropriate level of expertise must be applied to evaluate whether changes in the organization or infrastructure should trigger a change to the information security program. Changes that must be considered that could require an update to the information security program are the effect of changes in:

- Technology
- The sensitivity of the information
- The nature and extent of threats
- The company's business arrangements, e.g., mergers, alliances, joint ventures
- Customer information systems, e.g., new configurations, new connectivity, new software

5.6. Security Compliance Program

All relevant statutory, regulatory, and contractual requirements must be thoroughly researched, explicitly defined, and included in the current system documentation for every company's production information system. The company should establish the framework and assign roles and responsibilities to identify the relevant compliance requirements and maintain GatherAct's compliance with the specified requirements.

6. Violations

Any violation of this policy may result in disciplinary action up to and including termination of employment or contract. The company reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and cooperate in investigating such activity. The company does not consider conduct in violation of this policy within an employee's or partner's course and scope of employment or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, the company reserves the right not to defend or pay any damages awarded against employees or partners that result from violations of this policy.

Any employee or partner who is requested to undertake an activity that he or she believes violates this policy must provide a written or verbal complaint to his or her manager, any other manager as soon as possible.