Table of Contents

Table of Contents

Purpose

The purpose of this document is to describe SecurityGate's ICS (Industrial Control Domain) ICS Privacy and Data Handling Policy and Procedure program. All SecurityGate employees are responsible for protecting the company's assets, and the leadership, at every level, is explicitly accountable for ensuring employees understand and comply with ICS policies and procedures.

The objective of this program is to detail SecurityGate's policies and procedures regarding handling of personal information collected on the Platform. A further objective of this program is to detail the how to educate and make aware of the ICS cyber security risks and their responsibilities to all personnel, contractors and third parties who are involved with company's core business of` operations.

Policy Objective

The objective of the ICS Privacy and Data Handling Policy and Procedure Program is to identify the type of awareness and education training programs for each of the job roles within SecurityGate. This program should be compatible with existing IT programs and other (Industrial Control Domain) security programs that are currently in place.

The individual objective is that for each role, the person should have a level of understanding and competence of the security threats, risks and issues that could impact the safe running of the operations.

Program Definition

This plan will define the roles of the personnel involved in the Privacy and Data Handling Policy and Procedure program, and then the levels of competence will be defined, followed by a mapping of the roles and the levels.

Organizations should identify all PII residing in their environment. An organization cannot properly protect PII it does not know about. PII is —any information about an individual maintained by an agency, including

(1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and

(2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include, but are not limited to:

Name, such as full name, maiden name, mother‘s maiden name, or alias.

Personal identification number, such as social security number (SSN), passport number, driver‘s license number, taxpayer identification number, or financial account or credit card number.

Address information, such as street address or email address.

Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry).

How are entities stored on the platform?

Security Controls

The security controls in place for the SecurityGate SaaS Platform is SHA256 Encrpytion when data is at rest with Amazon Web Services.

In addition to the PII-specific safeguards described earlier in this section, many types of security controls are available to safeguard the confidentiality of PII. Providing reasonable security safeguards is also a Fair Information Practice.

Access Enforcement

SecurityGate can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).

Encrypting stored information is also an option for implementing access enforcement

Separation of Duties

SecurityGate enforces separation of duties on the SaaS Platform by implementating Role Based Access Control. There are four roles ranging from the User to Admin functions each with a specified and limited access to entities created on the SaaS Plattform. Organizations can enforce separation of duties for duties involving access to PII. For example, the users of de-identified PII data would not also be in roles that permit them to access the information needed to re-identify the records.

Least Privilege

SecurityGate can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. Concerning PII, SecurityGate can ensure that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

Remote Access

SecurityGate chooses to prohibit or strictly limit remote access to PII. If remote access is permitted, SecurityGate ensures that the communications are encrypted.

User-Based Collaboration and Information Sharing

SecurityGate can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually based restrictions, for PII.

Access Control for Mobile Devices

SecurityGate can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).

Auditable Events

SecurityGate can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.

Audit Review, Analysis, and Reporting

SecurityGate can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

Identification and Authentication (Organizational Users)

Users can be uniquely identified and authenticated before accessing PII. The strength requirement for the authentication mechanism depends on the impact level of the PII and the system as a whole.

Media Access

SecurityGate can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). This could also include portable and mobile devices with a storage capability.

Media Marking

SecurityGate can label information system media and output containing PII to indicate how it should be distributed and handled.

Media Storage

SecurityGate can securely store PII, in digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures. One example is the use of storage encryption technologies to protect PII stored on removable media.

Media Transport

SecurityGate can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas. Examples of protective safeguards are encrypting stored information and locking the media in a container.

Media Sanitization
SecurityGate can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.

Transmission Confidentiality
SecurityGate can protect the confidentiality of transmitted PII.

Protection of Information at Rest
SecurityGate can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.

Information System Monitoring

SecurityGate can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.

Incident Responses for Breaches involving PII

Handling incidents and breaches involving PII is different from regular incident handling and may require additional actions by SecurityGate. Due to particular risks of harm, SecurityGate may develop additional policies, such as determining when and how individuals should be notified, when and if a breach should be reported publicly, and whether to provide remedial services, such as credit monitoring, to affected individuals.

Add workflow diagram

SecurityGate's SSA (Subscription Services Agreement)

Data Security Measures:

Security Measures.

In order to protect Customer's Confidential Information, SecurityGate will:

(i) implement and maintain all reasonable security measures appropriate to the nature of the Confidential Information including without limitation, technical, physical, administrative and organizational controls, and will maintain the confidentiality, security and integrity of such Confidential Information;

(ii) implement and maintain industry standard systems and procedures for detecting, preventing and responding to attacks, intrusions, or other systems failures and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures;

(iii) designate an employee or employees to coordinate implementation and maintenance of its Security Measures (as defined below); and

(iv) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Customer's Confidential Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks (collectively, Security Measures).

Notice of Data Breach:

If SecurityGate knows that Customer Confidential Information has been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this agreement, SecurityGate will alert Customer of any such data breach without undue delay , and immediately take such actions as may be necessary to preserve forensic evidence and eliminate the because of the data breach. SecurityGate

will give highest priority to immediately correcting any data breach and devote such resources as may be required to accomplish that goal. SecurityGate will provide Customer with all information necessary to enable Customer to fully understand the nature and scope of the data breach. To the extent that Customer, in its sole reasonable discretion, deems warranted Customer may provide notice to any or all parties affected by any data breach. In such case, SecurityGate will consult with Customer in a timely fashion regarding appropriate steps required to notify third parties. SecurityGate will provide Customer with information about what SecurityGate has done or plans to do to minimize any harmful effect or the unauthorized use or disclosure of, or access to,

Confidential Information:

SecurityGate will determine if existing processes are adequate, and if not, establish a new incident reporting method for employees to report suspected or known incidents involving PII. The method could be a phone hotline, email, online form, or a management reporting structure in which employees know to contact a specific person within the management chain. Employees should be able to report any breach involving PII immediately on any day, at any time. Additionally, employees should be provided with a clear definition of what constitutes a breach involving PII and what information needs to be reported.

Plan for dealing with a Data Breach

Stop the breach

Once a breach is identified care must be taken to isolate the affected systems. Time is of the essence.

Assess the damage

The next step is to assess the damage to the organization.

Notify those affected

The next step is to notify authorities, third parties, and those affected.

Security audit

A security audit is needed to assess the organization's current security system and to prepare for future recovery plans.

Update your recovery plan to prepare for future attacks

The security audit and investigation will help to highlight vulnerabilities and give guidance towards revising the recovery plan.

Train our employees

Routine security and privacy training is a must.

Protect the data

All sensitive data must be protected. When disposing of physical storage, the data it contains will be shredded.

Enforce strong passwords

Enforce strong passwords throughout the organization, requiring change every 6 months.

Monitor data and its transfer

Monitoring and tracking the transfer of data through-out the company will prevent the data from being misused or exploited.

Limit access

Limit the access to certain systems by people who are not connected to the department, and make sure that sensitive data is handled only by relevant professionals.

Patch vulnerabilities

Out-of-date software and unattended vulnerabilities are often the vector of data breaches and should be patched in a timely matter.

Encrypt devices and data

SecurityGate shall not allow devices or data that are not encrypted, as they're more prone and vulnerable to attacks.

Two-factor authentication

Adding this additional layer of security will provide greater protection than using only password authentication.

Limit downloading

Restricting downloadable media will prevent the transferring of sensitive data to external devices.

Breach recovery plan

Responding to a breach needs to be fast and efficient. And having a strong breach recovery plan will minimize the damages a data breach can bring.

Privacy Shield Compliance

SecurityGate is engaged in self-certification to Privacy Shield and actively adheres to its principles.

This and other sections of this document are a collective of statements representing SecurityGate's commitment to be subject to the Principles for all personal data received from the EU in reliance on the Privacy Shield.

The purpose of this document is to describe SecurityGate's ICS (Industrial Control Domain) ICS Privacy and Data Handling Policy and Procedure program. All SecurityGate employees are responsible for protecting the company's assets, and the leadership, at every level, is explicitly accountable for ensuring employees understand and comply with ICS policies and procedures.

A further objective of this program is to detail the how to educate and make aware of the ICS cyber security risks and their responsibilities to all personnel, contractors and third parties who are involved with company's core business of` operations.

Personal information collected by SecurityGate

Personal information collected by SecurityGate is the information the client provides SecurityGate through the Platform.

This and other sections of this document are a collective of statements representing Our organization's commitment to be subject to the Principles for all personal data received from the EU in reliance on the Privacy Shield.

How SecurityGate uses personal information collected

The purpose for which personal data is collected would be for the creation of entity accounts and for assigning assessment workflows to the individuals on the Platform. SecurityGate uses personal information to measure, analyze performance, troubleshoot, provide support for, improve, and enhance the Platform. SecurityGate uses the personal information you provided to the Platform to communicate with you.

Access and Choice

SecurityGate provides mechanisms to allow you to access and delete personal information you provided to the Platform.

Location of Personal Information

The SecurityGate platform is hosted on AWS (Amazon Web Services, Inc.). The SecurityGate.io domain is hosted on GoDaddy. The Database is PostgreSQL. CUBA is the web development platform. Bitbucket is used to coordinate source code changes. The SecurityGate platform is backed up on AWS (Amazon Web Services, Inc.), daily. There are two different locations to provide uptime redundancy. All data is hosted in the continental United States.

Regarding File Storage, files are separated and stored in dedicated directories whose naming conventions are generated from schema-based, unique identifiers. That is, a unique, encrypted directory is created for each entity. The database and associated schema utilize a multi-tenancy model in which tables are shared while columns containing unique identifiers as well as encryption hashes allow for selective and secure retrieval of data. The platform utilizes AES 256-bit encryption to authenticate and verify every user session. These same methods are implored during all data transactions, allowing for said data (and transaction) to only be linked to the given, authenticated entity. These unique, authenticated identifiers are applied at both the Customer and individual User level.

Retention of Personal Information

SecurityGate retains personal information for the purpose of providing access and services on the Platform. We will delete your personal information in accordance with any applicable law.

How to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints.

SecurityGate

5400 Katy Freeway

Houston, Texas 77007

The type or identity of third parties to which it discloses personal information, and the purposes for which it does so.

SecurityGate stores SaaS Platform data on Amazon Web Services Cloud infrastructure.

Individuals have the right to access their personal data.

There is also the possibility, under certain conditions, for the individual to invoke binding arbitration, SecurityGate realizes it has the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and its liability in cases of onward transfers to third parties.

Notice

This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the SecurityGate Platform or as soon thereafter as is practical, but in any event before the SecurityGate uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

Choice

SecurityGate must offer individuals the opportunity to choose (opt out) whether their personal information is

(i) to be disclosed to a third party or

(ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

Accountability for onward Transfer

To transfer personal data to a third party acting as an agent, SecurityGate must:

(i) transfer such data only for limited and specified purposes;

(ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles;

(iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the SecurityGate's obligations under the Principles;

(iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; take reasonable and appropriate steps to stop and remediate unauthorized processing;

(v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; including under (iv), and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

Security

SecurityGate maintains the security of personal information through a mix of best practice technologies for securing data at rest, data in use, and data in transit. Encryption, authentication, and hashing technologies are implemented to secure personal information.

Data Integrity and Purpose Limitation

Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. SecurityGate may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual.

Access

SecurityGate in creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data. SecurityGate acknowledges that individuals have the right to access their personal data submitted to the Platform.

Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. SecurityGate may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, SecurityGate must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. SecurityGate must adhere to the Principles for as long as it retains such information.
SecurityGate should take reasonable and appropriate measures in complying with this provision.

Recourse Mechanisms

i. SecurityGate must respond to a consumer within 45 days of receiving a complaint. The recourse available to individuals is readily available and free of charge to individuals.

ii. Independent recourse mechanisms must include on their public websites information regarding the Privacy Shield Principles and the services that they provide under the Privacy Shield. This information must include:

(1) information on or a link to the Privacy Shield Principles' requirements for independent recourse mechanisms;

(2) a link to the Department's Privacy Shield website;

(3) The dispute resolution services under the Privacy Shield are free of charge to individuals;

(4) a description of how a Privacy Shield-related complaint can be filed;

- Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the arbitration panel with respect to remedies. In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney's fees.
- Consistent with applicable law, within 6 months from the adoption of the adequacy decision, the Department of Commerce and the European Commission will agree to adopt an existing, well-established set of U.S. arbitral procedures (such as AAA or JAMS) to govern proceedings before the Privacy Shield Panel, subject to each of the following considerations:
- An individual may initiate binding arbitration, subject to the pre-arbitration requirements provision above, by delivering a "Notice" to the organization. The Notice shall contain a summary of steps taken under Paragraph C to resolve the claim, a description of the alleged violation, and, at the choice of the individual, any supporting documents and materials and/or a discussion of law relating to the alleged claim.

- Procedures will be developed to ensure that an individual's same claimed violation does not receive duplicative remedies or procedures.
- FTC action may proceed in parallel with arbitration.
- No representative of the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority may participate in these arbitrations, provided, that at the request of an EU individual, EU DPAs may provide assistance in the preparation only of the Notice but EU DPAs may not have access to discovery or any other materials related to these arbitrations.
- The location of the arbitration will be the United States, and the individual may choose video or telephone participation, which will be provided at no cost to the individual. In-person participation will not be required.
- The language of the arbitration will be English unless otherwise agreed by the parties. Upon a reasoned request, and taking into account whether the individual is represented by an attorney, interpretation at the arbitral hearing as well as translation of arbitral materials will be provided at no cost to the individual, unless the panel finds that, under the circumstances of the specific arbitration, this would lead to unjustified or disproportionate costs.
- Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
- Individual-specific discovery may be permitted if necessary, and such discovery will be treated confidentially by the parties and will only be used in connection with the arbitration.
- Arbitrations should be completed within 90 days of the delivery of the Notice to the organization at issue, unless otherwise agreed to by the parties.

iii. Independent recourse mechanisms must publish an annual report providing aggregate statistics regarding their dispute resolution services. The annual report must include:

(1) the total number of Privacy Shield-related complaints received during the reporting year;

(2) the types of complaints received;

(3) dispute resolution quality measures, such as the length of time taken to process complaints; and

(4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed.

iv. As set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is

available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles or with respect to an allegation about the adequacy of the Privacy Shield. Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.

e. Remedies and Sanctions

i. The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, insofar as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances. Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of Privacy Shield organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department.

*****

5. Section I.5 of the Principles.
6. Dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used, or disclosed information in blatant contravention of the Privacy Shield Principles.

Self-Certification Information

Information Required for Privacy Shield Self-Certification

Organization Information:

- Organization Name: SecurityGate
- Address: 5400 Katy Freeway
- City: Houston
- State: Texas
- Zip: 77007

Organization Contact: Provide a contact office and individual within your organization for the handling of complaints, access requests, and any other issues concerning your organization's compliance with the Privacy Shield Framework.

- Contact Office: Houston
- Contact Name: Brent Gage
- Contact Title: ICS Security SME
- Contact E-mail: Brent@securitygate.io
- Contact Phone: 254.717.1188
- Contact Fax

Organization Corporate Officer: Provide information about the individual certifying your organization's compliance with the Privacy Shield Framework. By submitting this self-certification, the corporate officer attests that he/she is authorized to submit the self-certification on behalf of your organization and all entities or subsidiaries indicated below.

- Corporate Officer Name: Ted Gutierrez
- Corporate Officer Title: CEO
- Corporate Officer E-mail: ted@securitygate.io
- Corporate Officer Phone: 713.344.6351
- Corporate Officer Fax

Privacy Shield List https://www.privacyshield.gov/list

https://www.securitygate.io/privacy-shield

Statement of participation in Privacy Shield

SecurityGate is engaged in self-certification to Privacy Shield and actively adheres to its principles.

This and other sections of this document are a collective of statements representing SecurityGate's commitment to be subject to the Principles for all personal data received from the EU in reliance on the Privacy Shield.

The purpose of this document is to describe SecurityGate's ICS (Industrial Control Domain) ICS Privacy and Data Handling Policy and Procedure program. All SecurityGate employees are responsible for protecting the company's assets, and the leadership, at every level, is explicitly accountable for ensuring employees understand and comply with ICS policies and procedures.

A further objective of this program is to detail the how to educate and make aware of the ICS cyber security risks and their responsibilities to all personnel, contractors and third parties who are involved with company's core business of` operations.

Ted Gutierrez CEO SecurityGate

References

4.1. NIST Special Publication 800-122

4.2. Privacy Shield Framework documentation.

4.3. ICS Framework on SecurityGate's Intranet site

4.3.1. ICS Framework RACI Matrix

4.3.2. ICS Deviation Policy and Procedure

4.4. Industrial Control Domain – Security Requirements for Vendors

(Version History

Version No.	Date	Description of Change	By
1.0	December 20, 2019	Final Version	Mick Vaughan

Document Approval

Reviewers	Title	Signature	Date	Comments