




■ PRITS-POL-0009

## Privacy Policy

- Application: All
- System: All

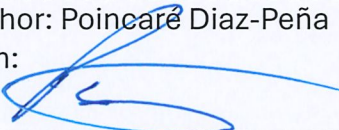


Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

## Table of Contents

1. Description.....	3
2. Legal Basis .....	3
4. Scope .....	4
5. Abbreviations, Acronyms, Definitions, and Meanings .....	4
6. Policy .....	7
7. Responsibilities.....	11
8. Penalties.....	12
9. Policy Training & Delivery Process .....	12
10. Exemption Request.....	13
11. Effective Period .....	13
12. References.....	13
13. Approval Signatures.....	15
14. Revision History .....	16



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Diaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

## 1. Description

This policy establishes the principles, responsibilities, and minimum standards for protecting personal data collected, processed, stored, or shared by the Puerto Rico Innovation and Technology Service (PRITS). It applies to all individuals whose personal data is handled by the agency while providing public services, operating IT systems, or managing internal operations. The policy reflects PRITS' commitment to respecting privacy rights and ensuring transparency, accountability, and lawful data processing.

## 2. Legal Basis

This policy is issued pursuant to Law No. 75-2019, known as the "Puerto Rico Innovation and Technology Service (PRITS) Act," and Law No. 40-2024, known as the "Commonwealth of Puerto Rico Cybersecurity Act."

Law No. 75-2019, *supra*, establishes PRITS as responsible for public policy regarding the management, development, and integration of the Government's technological infrastructure, in addition to creating strategies and standards for information technologies.

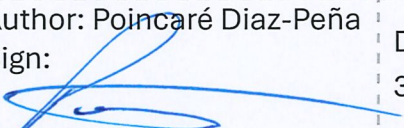
For its part, Law No. 40-2024, *supra*, defines a legal framework to strengthen cybersecurity in the Government, protecting data, networks, and critical infrastructure, and promoting citizen privacy and compliance with federal regulations, with sanctions for non-compliance.

## 3. Purpose

The purpose of this policy is to:

- Define how PRITS collects, uses, stores, and protects personal information.
- Ensure compliance with applicable privacy laws and regulations.
- Minimize the risk of unauthorized access, misuse, or disclosure of Personally Identifiable Information (PII).
- Promote trust among users, stakeholders, and employees in the agency's data handling practices.



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

#### 4. Scope

This policy applies to:

- All PRITS employees, contractors, consultants, and third parties with access to personal data handled by PRITS.
- All systems, applications, and processes used to collect or manage personal information.
- All types of personal data, regardless of whether it is processed digitally or manually.

The policy covers data collected from internal and external users, including:

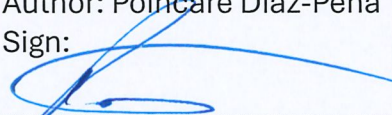
- Agency personnel
- Citizens and service recipients
- Vendors and partners

#### 5. Abbreviations, Acronyms, Definitions, and Meanings

Abbreviation / Acronym	Meaning
CIIO	Chief Innovation and Information Officer
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
PII	Personally Identifiable Information
MFA	Multi-Factor Authentication
PRITS	Puerto Rico Innovation and Technology Service
RBAC	Role-Based Access Control

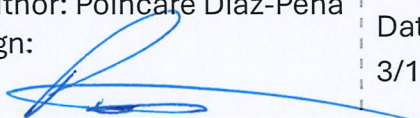
Term	Definition
Access	The ability or means necessary to read, write, modify, or communicate data/information or use any system resource.
Anonymization	A process that de-associates the dataset and the data subject.
Authorization	The process of granting a user access privileges to information or an information system following the Principle of Least Privilege.
Credentials	Unique attributes provided to each authorized user to access information system resources and applications.



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

Term	Definition
Data	Any sequence of one or more symbols that are given meaning by specific acts of interpretation.
Data Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: <ul style="list-style-type: none"> <li>- a person other than an authorized user accesses or potentially accesses personally identifiable information;</li> <li>- or an authorized user accesses personally identifiable information for another than authorized purpose.</li> </ul>
Data Minimization	The principle that personal data collected should be limited to what is necessary in relation to the purposes for which it is processed.
Data Subject	An individual whose personal data is collected, held, or processed.
Encryption	Cryptographic transformation of readable data (plaintext) to an unreadable form (ciphertext) to protect its confidentiality, preventing its knowledge or use by unauthorized users. If this transformation is reversible, the reverse process is called decryption, which restores the data to its original state.
Government	The Commonwealth of Puerto Rico.
Information System	A discrete set of information resources for the collection, processing, maintenance, use, exchange, dissemination, or disposition of information.
Least Privilege Principle	Each module (process, user, or program, depending on the topic) can only access the information and resources necessary for its legitimate purpose.
Log	A record of events occurring across an organization's systems and networks.
Personally identifiable information (PII)	Any representation of information that is readable without the need for a special cryptographic key to access it or that facilitates the tracing of an individual's identity, including the name or first initial and last name of an individual combined with other information that is linked or likely to be linked to a specific individual, such as: <ul style="list-style-type: none"> <li>- Social Security number</li> <li>- Driver's license number, voter registration card, or other government-issued ID</li> <li>- Bank or financial account numbers of any kind, with or without access codes</li> <li>- Usernames and passwords for access to public or private computer systems</li> <li>- HIPAA-protected health información</li> </ul>

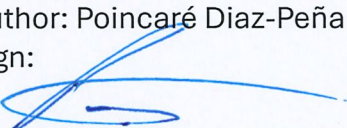


Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

Term	Definition
	<ul style="list-style-type: none"> <li>- Tax information</li> <li>- Job evaluations</li> </ul> <p>For purposes of this Policy, the terms 'personal data,' 'personal information,' and 'personally identifiable information' shall be used interchangeably.</p>
PRITS	Puerto Rico Innovation and Technology Service, Executive Branch Office in charge of implementing, developing, and coordinating the Government's public policy on innovation, information, and technology, as provided by Law 75 of 2019.
Privacy	The right of individuals to control or influence how their personal data may be collected, used, stored, shared, or disclosed, and under what circumstances. It encompasses the ability to maintain autonomy over personal data and to safeguard it from unauthorized access, misuse, or surveillance.
Risk	Any reasonably identifiable circumstance or event that potentially adversely affects the security of networks and information resources.
Role-based access control (RBAC)	Set of authorizations granted to a user upon assuming a role, either explicitly or implicitly. The permissions of a role can be inherited through role hierarchy and typically reflect the permissions necessary to perform specific functions within an organization. The same role can be assigned to one or more individuals.
Unauthorized access	Occurs when a person, group, code, program, application, or any other entity or computing process obtains logical, digital, or physical access without approval or consent to a critical infrastructure network, system, data, application, "data room," or other Government information technology resource, or when access is obtained or attempted to be obtained to information or resources that are not necessary to fulfill their job or function, following the Principle of Least Privilege.
User	An individual or (system) process authorized to access an information system.

This space has been intentionally left blank.



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

## 6. Policy

### 6.1 Lawful, Fair, and Transparent

- 6.1.1 Personal data shall be collected and processed only when there is a clear legal basis or legitimate governmental need. This includes the performance of public duties, legal obligations, or tasks carried out in the public interest.
- 6.1.2 Individuals shall be informed of why their data is being collected, how it will be used, and with whom it may be shared.
- 6.1.3 Consent, where required, must be freely given, specific, informed, unambiguous, and documented, following applicable legal regulations.

### 6.2 Purpose Limitation and Data Minimization

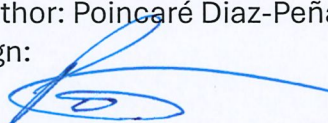
- 6.2.1 Personal data shall only be used for specific, explicit, and legitimate purposes for which it was collected. Any further processing must be compatible with this original purpose or supported by a lawful basis.
- 6.2.2 PRITS shall evaluate and define the minimum personal data required to perform each service or function, ensuring that data collection efforts are narrowly tailored and justifiable.
- 6.2.3 Data shall not be used for unrelated or new purposes without obtaining the necessary legal authority or informed consent from the data subject, as applicable.
- 6.2.4 All data collection processes shall be subject to periodic review to confirm continued necessity and relevance.

### 6.3 Accuracy

- 6.3.1 PRITS shall implement reasonable mechanisms to ensure that personal data is accurate, complete, and up to date.
- 6.3.2 Individuals shall have the right to review and request the correction or amendment of inaccurate, incomplete, or outdated personal data, subject to verification and following applicable legal procedures, before the agency(ies) that originally produced or controlled the personal data.
- 6.3.3 Where data inaccuracies are identified, PRITS will take prompt and reasonable steps to correct or delete the information as appropriate, if the data was originally produced or controlled the personal data.

### 6.4 Storage Limitation



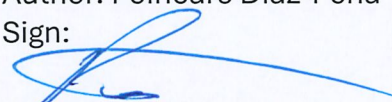
Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

- 6.4.1 Personal data shall be retained only for as long as it is necessary to fulfill the specified purpose(s) for which it was collected or as otherwise required by law, regulation, or an authorized records retention schedule.
- 6.4.2 Upon expiration of the retention period or fulfillment of the purpose, data shall be securely deleted, destroyed, or rendered irreversibly anonymized.
- 6.4.3 Exceptions to retention limits must be documented, justified under law, and subject to approval by a designated data governance authority within PRITS.

## 6.5 Security of Processing

- 6.5.1 Appropriate technical and organizational security measures shall be implemented to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These measures include, but are not limited to:
  - 6.5.1.1 Role-Based Access Controls (RBAC)  
Access to personal data shall be restricted to personnel with a legitimate need to know, based on their job responsibilities, as stated in the Identity, Credentials, and Access Management Policy (PRITS-POL-0004).
  - 6.5.1.2 Secure Transmission Protocols  
All electronic data transfers involving personal information shall be encrypted using secure protocols (e.g., TLS, HTTPS), as established in the Encryption and Cryptographic Controls Policy (PRITS-POL-0003).
  - 6.5.1.3 Endpoint Protection  
Devices accessing or storing personal data must have up-to-date antivirus software, firewalls, and device management controls.
  - 6.5.1.4 Physical Safeguards  
Printed records and physical media containing personal data must be stored in secured environments with access logs, locks, and restricted entry.
  - 6.5.1.5 Multi-Factor Authentication (MFA)  
Systems housing sensitive personal data shall require multi-factor authentication to access as required by the Identity, Credentials, and Access Management Policy (PRITS-POL-0004).



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

6.5.2 Regular security audits and vulnerability assessments shall be conducted to identify and mitigate potential data integrity and confidentiality risks.

6.5.3 All staff and contractors must complete mandatory cybersecurity and data privacy training annually to ensure awareness of current threats and safe data handling practices.

## 6.6 Data Sharing and Disclosure

6.6.1 Personal data may be disclosed to third parties only under the following circumstances:

### 6.6.1.1 Legal Requirements

When required by law, regulation, court order, subpoena, or other legal process.

### 6.6.1.2 Service Provision

When necessary to deliver a public service or perform a contract or agreement on behalf of PRITS, provided that the receiving party is contractually bound to protect the data.

### 6.6.1.3 Informed Consent

When explicit consent has been obtained from the individual, unless otherwise permitted or required by law.

6.6.2 Third parties or service providers who receive personal data from PRITS must be contractually obligated to:

6.6.2.1 Use the data solely for the purposes for which it was disclosed.

6.6.2.2 Implement data protection measures equivalent to or exceeding PRITS' standards.

6.6.2.3 Promptly report any suspected or confirmed data breaches or unauthorized disclosure involving PRITS data.

6.6.3 PRITS shall maintain an e-register of all third-party data-sharing agreements either and/or rely on the Register of Contracts in the Office of the Comptroller.

6.6.4 Under no circumstances shall PRITS sell, lease, or trade personal data to external entities for solely for commercial or marketing purposes.

## 6.7 Data Breaches

6.7.1 All personnel and contracted service providers are required to report suspected or actual data breaches immediately to the Computer Security Incident Response Team (CSIRT-PRITS) through established



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025
Sign:		

reporting channels as required by the Information Security Incident Response Policy (PRITS-POL-0002).

- 6.7.2 All staff and contractors shall receive recurring training on identifying, preventing, and responding to data breaches as part of PRITS' broader information security awareness program.

## 6.8 Data Subject Rights

### 6.8.1 Right to Access

Individuals have the right to request access to their personal data held by PRITS. Upon verification of identity, PRITS shall provide a copy of the requested information, including the purposes of processing, categories of data processed, and any third parties with whom the data has been shared.

### 6.8.2 Right to Rectification

Individuals may request the correction or amendment of inaccurate, incomplete, or outdated personal data, subject to verification and following applicable legal procedures, before the agency(ies) that originally produced or controlled the personal data.

### 6.8.3 Right to Restriction of Processing

Individuals have the right to request a temporary or permanent halt to processing their data under certain conditions, such as during a dispute over data accuracy or processing legality.

### 6.8.4 Right to Object

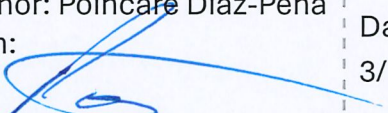
Where personal data is processed based on public interests, an individual may object to the processing on grounds relating to their specific situation. PRITS shall evaluate such objections following legal requirements.

### 6.8.5 Right to Data Portability

If applicable, individuals may request to receive their personal data in a structured, commonly used, and machine-readable format or to have that data transmitted to another entity, where technically feasible.

### 6.8.6 Right to Withdraw Consent



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

If processing is based on the individual's consent, that consent can be withdrawn at any time. Withdrawal shall not affect the lawfulness of prior processing.

## 7. Responsibilities

### 7.1 Chief Information Security Officer (CISO)

- 7.1.1 Serves as the executive lead for privacy and data protection strategy.
- 7.1.2 Oversee the integration of privacy and security controls into agency-wide systems, applications, and operations.
- 7.1.3 Coordinates response to data breaches and ensures appropriate reporting and remediation activities.

### 7.2 Cybersecurity Team / Computer Security Incident Response Team (CSIRT-PRITS)

- 7.2.1 Implement and monitor technical safeguards to secure personal data against unauthorized access or disclosure.
- 7.2.2 Investigate suspected or confirmed data breaches and supports containment, remediation, and recovery efforts.
- 7.2.3 Ensure data protection controls (e.g., encryption, RBAC, MFA) are applied following agency policies.

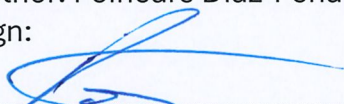
### 7.3 Legal Office

- 7.3.1 Provide legal interpretation of applicable data protection and privacy laws, regulations, and standards.
- 7.3.2 Review and approve data-sharing agreements, third-party contracts, and consent forms for legal sufficiency.
- 7.3.3 Advice on lawful bases for data processing and assists in responding to complaints or legal challenges from data subjects.

### 7.4 System Owners / Program Managers

- 7.4.1 Identify and document all personal data collected, processed, and stored within their systems.
- 7.4.2 Ensure compliance with data minimization, accuracy, and retention requirements.



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

7.4.3 Coordinate with the cybersecurity and legal teams to implement appropriate safeguards.

## 7.5 All PRITS Personnel and Contractors

- 7.5.1 Must adhere to the privacy principles and practices outlined in this policy.
- 7.5.2 Participate in required privacy, data protection, and information security training.
- 7.5.3 Report any suspected or actual data breaches or policy violations through the appropriate channels.
- 7.5.4 Collect, use, and disclose personal data only as authorized and consistent with job responsibilities.

## 8. Penalties

Non-compliance with this Policy may result in suspension of system access, disciplinary actions, and/or contract termination, as appropriate.

## 9. Policy Training & Delivery Process

To ensure that all employees and contractors whose scope of work is related to this Policy understand and comply with it, PRITS establishes the following Training & Delivery Process.


### 9.1 Initial Policy Distribution

This Policy will be disseminated to all employees via official PRITS communication channels (email, intranet, or employee portal). A copy of this Policy will be available at the Chief Information Security Office.

### 9.2 Employee Acknowledgment

All employees and contractors whose work is relevant to this Policy must acknowledge receipt and review it. PRITS shall determine the acknowledgment method for record-keeping purposes.



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Díaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

Acknowledgment is mandatory for all new employees/contractors upon onboarding and for existing employees/contractors upon major policy updates.

### 9.3. Training, Skill and Proficiency

All individuals covered by this Policy shall receive initial training and introduction to this Policy. PRITS shall continue to readdress the extent of this Policy with the covered individuals annually or in shorter intervals if changes in this policy warrant it.

### 9.4. Policy Updates & Acknowledgment

Any major revisions to this Policy will require employees/contractors to review and acknowledge changes within 15 days of notification.

Updated policies will be delivered via email, intranet, or compliance training platforms.

## 10. Exemption Request

If compliance with this policy proves unfeasible or technically impossible, or an exception is required, the system owner or administrator must submit a formal written request to the CISO and the CIO. This request must be sent to the email address [cumplimentocyber@prits.pr.gov](mailto:cumplimentocyber@prits.pr.gov).


## 11. Effective Period

This policy will be effective immediately.

## 12. References

Identification Number	Title	Version
ISO/IEC 27001	Information Security Management Systems (ISMS)	Ed. 3
ISO/IEC 27701	Extension to Privacy Information Management	Ed. 1

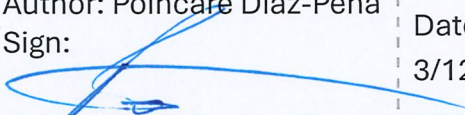


Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>
Author: Poincaré Diaz-Peña Sign: 	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025

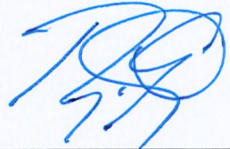
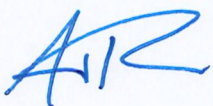
Identification Number	Title	Version
Law No. 40-2024	Commonwealth of Puerto Rico Cybersecurity Act	N/A
Law No. 75-2019	Puerto Rico Innovation and Technology Service Act	N/A
PRITS-POL-0002	Information Security Incident Response Policy	1.0
PRITS-POL-0003	Encryption and Cryptographic Controls Policy	1.0
PRITS-POL-0004	Identity, Credentials, and Access Management Policy	1.0

This space has been intentionally left blank.



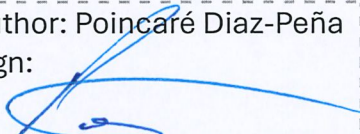
Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>	
Author: Poincaré Díaz-Peña	Date: 3/12/2025	Status: Approved Version: 1.0 Effective date: 3/12/2025	
Sign: 			

### 13. Approval Signatures

Position	Action Taken	Print Name	Signature	Date
Chief Technology Officer	Revised by	Rubén Quiñones-Millán		3/12/2025
Chief Innovation and Information Officer	Approved by	Antonio Ramos-Guardiola		3/12/2025

This space has been intentionally left blank.



Title: Privacy Policy		Number: <b>PRITS-POL-0009</b>	
Author: Poincaré Díaz-Peña	Date: 3/12/2025	Status: Approved	
Sign: 		Version: 1.0 Effective date: 3/12/2025	

#### 14. Revision History

Version	Date	Author	Change Description

This space has been intentionally left blank.