RPACT Information Security Policy

RPACT GmbH

POL-RPACT-007

Version 1.0.0

Contents

RPACT GmbH

Am Rodenkathen 11
23611 Sereetz
Germany
www.rpact.com

Policy ID	POL-RPACT-007
Title	RPACT Information Security Policy
Description	This policy defines RPACT GmbH's information security principles and controls for protecting the confidentiality, integrity, and availability of RPACT, client, and project information across systems, documentation, software development, collaboration, and service delivery activities.
Author	Friedrich Pahlke
Reviewer	Gernot Wassmer, Daniel Sabanés Bové
Creation date	2026-01-19
Version	1.0.0
Date of modification	2026-01-19
Effective date	2026-01-19

1 Purpose

This policy defines RPACT GmbH's overall approach to information security. It establishes the principles and controls used to protect the confidentiality, integrity, and availability of RPACT information assets, client information, software, documentation, repositories, cloud-based services, and project records.

This policy serves as the overarching information security policy for RPACT and is supported by the more specific policies referenced in the section *Related Policies*.

2 Scope

This policy applies to all information, systems, software, documentation, repositories, collaboration platforms, and cloud services created, used, or managed by RPACT GmbH. It applies to the RPACT partners, independent collaborators, and any future employees or contingent workers.

The scope includes internal tools, validated or client-facing software, project records, source code, system documentation, client information, and information processed in connection with RPACT products and services such as rpact and RPACT Cloud.

3 Company Context

RPACT GmbH is structured as a small partnership of highly specialized professionals. Core work is performed by the partners and trusted external experts under formal confidentiality obligations. RPACT does not operate a large internal IT department or an on-premise data center. Instead, RPACT uses risk-appropriate, access-controlled cloud and collaboration services, including version-controlled repositories, to manage software, documentation, and project records.

The information security controls defined in this policy are proportionate to RPACT's size, operating model, product architecture, and regulatory and client expectations. For GxP-relevant or client-critical work, additional validation, traceability, and review controls are applied as required.

4 Responsibilities

- The RPACT partners are jointly responsible for defining, implementing, reviewing, and enforcing information security practices.
- Each partner is responsible for protecting information assets under their control and for ensuring that security-relevant decisions are documented in a proportionate manner.
- External collaborators must work under an appropriate agreement, follow RPACT policies relevant to their role, and protect confidential information on a need-to-know basis.
- Future employees or contingent workers will receive role-appropriate onboarding and security awareness training before receiving access to RPACT systems or client information.

5 Information Security Principles

RPACT applies the following information security principles:

- **Confidentiality:** Information is accessed only by authorized persons with a legitimate business or project need.
- **Integrity:** Information, code, documentation, and configuration are protected against unauthorized or unintended modification.
- **Availability:** Information and systems required for service delivery are maintained in a manner that supports reliable access and recovery appropriate to their risk and criticality.
- **Least privilege:** Access rights are limited to the minimum necessary for the assigned role or task.
- **Accountability:** Activities are performed using individual accounts where possible, and security-relevant changes are traceable through version control, repository history, or other appropriate records.
- **Risk-based proportionality:** The depth and formality of security controls are adjusted to the sensitivity of the information, the criticality of the system, and applicable regulatory or client expectations.
- **Secure by design:** Security considerations are incorporated into software development, change management, supplier management, and documentation practices from the beginning of relevant activities.

6 Information Classification and Handling

RPACT classifies information according to its sensitivity and applies handling controls accordingly:

Classification	Examples	Handling Requirements
Public	Public website content, public package documentation, public release notes	May be shared externally after review and approval where appropriate
Internal	Internal procedures, planning notes, non-public project coordination	Shared only within RPACT or with authorized collaborators
Confidential	Source code in private repositories, contracts, commercial information, credentials-related metadata	Stored only in access-controlled systems and shared on a need-to-know basis
Client or Regulated Information	Client-provided information, GxP-relevant records, project-specific confidential information	Handled according to contractual, regulatory, and client-specific requirements; unnecessary local storage is avoided

- Client or regulated information must not be included in public repositories, public issue trackers, public documentation, or public support discussions.
- Secrets, passwords, access tokens, license keys, and private credentials must not be stored in source code, documentation, issue descriptions, or commit history.
- Sensitive information is shared only through approved, access-controlled channels and only to the extent required for the relevant task.
- Local copies of confidential or client information are avoided where possible and removed when no longer needed.

7 Access Control

7.1 User Access Management

- Access to repositories, documentation, systems, and collaboration platforms is granted only to authorized persons with a legitimate business or project need.
- Access is reviewed periodically and when responsibilities change.
- Access is revoked when a collaborator, employee, or other authorized user no longer requires access.
- Shared accounts are avoided where technically feasible; individual accounts are used to preserve traceability and accountability.

7.2 Authentication

- Access to security-relevant systems and repositories must be protected by strong authentication mechanisms.
- Multi-factor authentication or two-factor authentication is required for core collaboration and repository platforms where supported.
- Credentials must be kept confidential and must not be shared between users.
- Any suspected credential compromise must be reported immediately to the RPACT partners and addressed without undue delay.

7.3 Privileged Access

- Administrative or owner-level access is limited to the RPACT partners or explicitly authorized persons.

- Privileged access is used only when necessary for administration, release, security, or support activities.

- Changes performed with privileged access are documented through version control, platform audit history, or other appropriate records where available.

8 Remote Work and Physical Environment

RPACT operates primarily as a virtual workforce. Work is performed from private home offices or other controlled environments appropriate to the sensitivity of the work being performed.

- Confidential or client information must not be discussed or displayed where it can be viewed or overheard by unauthorized persons.

- Devices used for RPACT work must be protected by account-level access controls and reasonable physical safeguards.

- Devices must be locked when unattended.

- Public or shared workspaces may be used only when appropriate safeguards are in place and the activity does not expose confidential or client information.

- Paper records are avoided. If printed confidential information is used, it must be protected from unauthorized access and securely destroyed when no longer needed.

9 System and Software Security

RPACT applies security controls throughout the development and maintenance lifecycle of its software and information systems.

- Source code and technical documentation are maintained in version-controlled, access-controlled repositories.

- Changes to code, documentation, and configuration are documented and approved in accordance with RPACT's change and configuration management process.

- Secure coding and code review practices are applied in proportion to the architecture, data handling, and exposure of each application.

- Pull Requests, peer review, automated testing, and CI/CD checks are used where appropriate to support quality, traceability, and integrity.

- Dependencies and third-party components are reviewed in a risk-based manner, with particular attention to security-relevant or GxP-relevant components.

- Production releases or externally delivered versions require approval by at least one RPACT partner.

10 Data Storage, Transmission, and Retention

- RPACT information assets are stored in secure, access-controlled systems such as private repositories, approved cloud services, or controlled documentation platforms.
- Information transmitted electronically must use secure channels provided by the relevant platform, such as HTTPS, SSH, or equivalent protected transport mechanisms.
- Confidential and client information is retained only as long as required for contractual, regulatory, operational, or legitimate business purposes.
- Obsolete documents and records are archived or removed in accordance with the applicable document management and project requirements.
- Where client-specific retention or deletion requirements apply, they take precedence over internal default practices.

11 Logging, Monitoring, and Traceability

- Security-relevant actions are made traceable where supported by the platform, for example through repository history, Pull Request reviews, audit trails, issue history, release records, or documentation change history.
- Logs and trace records must not intentionally contain passwords, access tokens, private credentials, or unnecessary sensitive client information.
- Monitoring and log review are performed in a risk-based manner, focusing on systems or activities with security, client, or regulatory relevance.

12 Backup, Recovery, and Availability

- Critical source code, documentation, and project records are maintained in version-controlled or otherwise recoverable systems.
- Repository history, release tags, archived documents, and controlled change records support recovery to a known stable state.
- For critical or potentially disruptive changes, the standard back-out approach defined in RPACT's Change & Configuration Management Policy is applied.
- Availability and recovery expectations for client-specific work are addressed according to the applicable contract, project documentation, or service arrangement.

13 Third-Party and Supplier Security

RPACT uses third-party and supplier services only where appropriate for the business, development, documentation, or service delivery purpose.

- Third parties with access to RPACT systems, confidential information, or client information must operate under an appropriate formal agreement.
- Suppliers and collaborators are evaluated in a risk-based manner before and during engagement.
- Third-party access is limited to the minimum required and revoked when no longer needed.
- Client-specific information security or regulatory obligations are communicated to relevant third parties where applicable.

14 Security Awareness and Training

- Partners and collaborators must be familiar with RPACT policies relevant to their responsibilities.
- Security awareness is included in onboarding for new collaborators, employees, or contingent workers.
- Project-specific or client-specific security training is completed and documented where required.
- Security-relevant lessons learned from incidents, audits, reviews, or client feedback are incorporated into future training or process updates where appropriate.

15 Information Security Incident Management

An information security incident is any actual or suspected event that could compromise the confidentiality, integrity, or availability of RPACT systems, software, documentation, client information, credentials, or project records.

Examples include suspected unauthorized access, credential compromise, loss of a work device containing confidential information, accidental disclosure, malware, unauthorized changes, or public exposure of confidential information.

15.1 Reporting and Escalation

- Suspected information security incidents must be reported to the RPACT partners without undue delay.

- The partners assess the potential impact, affected information, affected clients or systems, and required containment actions.

- If client information or client systems may be affected, the relevant client contact is informed in accordance with contractual, regulatory, and legal obligations.

15.2 Response and Documentation

- Incident response actions may include containment, credential rotation, access revocation, restoration from a known stable state, correction of exposed information, and additional review or monitoring.

- Security incidents and significant suspected incidents are documented with the date, description, affected systems or information, actions taken, outcome, and any preventive measures.

- Lessons learned are reviewed by the partners and incorporated into policies, procedures, training, or technical controls where appropriate.

16 Exceptions

Given RPACT's small-company structure, information security controls are implemented using a streamlined and risk-based approach rather than a large, centralized information security management organization. RPACT does not maintain a dedicated security operations center or a separate internal IT security department.

Any exception to this policy must be justified, approved by at least one RPACT partner, and documented in a manner proportionate to the associated risk. Exceptions affecting client information, GxP-relevant work, or contractual security requirements require additional review and, where applicable, client agreement.

17 Related Policies

This policy is supported by the following RPACT policies:

- POL-RPACT-001 Document Management Policy

- POL-RPACT-002 Systems Development Policy

- POL-RPACT-003 Secure Coding & Code Review Policy

- POL-RPACT-004 Change & Configuration Management Policy

- POL-RPACT-005 Personnel Qualification and Training Policy

- POL-RPACT-006 Third Party and Supplier Management Policy

18 Review of Policy

This policy is reviewed annually or following significant changes to RPACT's systems, services, organizational structure, regulatory expectations, client requirements, or information security risk profile.

Approved by:

Dr. Friedrich Pahlke
Dr. Daniel Sabanés Bové

Date: *2026-01-19*
