

03. Information Security

▶ AT A GLANCE

- Our Information Security program, run by the Global Security Office (GSO), is aligned with the ISO 27001 framework to address our and our clients' security requirements.
- Violation of any security policy is a security breach.
- Publicis Groupe has comprehensive business continuity and disaster recovery plans.

WHY?

Within Publicis Groupe, protecting information for both the company and its clients is everyone's responsibility. A formal Information Security program has been established to meet the security requirements of Publicis Groupe and its clients.

FOR WHOM?

Publicis Groupe's Information Security policies are applicable to all employees, temporary workers, interns, and other personnel within Publicis Groupe, its Agencies, Business Units, Shared Service Centers (SSC), as well as authorized third parties such as freelancers, contractors, consultants, and suppliers.

For the purposes of this document, these individuals are collectively referred to as "People".

Additionally, Publicis Groupe and its agencies – including Business Units and SSC – are collectively designated as "Publicis Groupe" within this policy.

WHAT?

Publicis Groupe has adopted the following principles and objectives to provide and promote security:

Security Principles

1. Ethical Responsibility

Uphold the rights and interests of Publicis Groupe, its clients and People through responsible and ethical application of security measures.

2. Transparency

Maintain openness in the design and implementation of security objectives, ensuring clarity in purpose and execution.

3. Risk-Based Approach

Align security controls proportionally with assessed or anticipated risks to ensure appropriate and efficient protection.

4. Accountability

Promote clear ownership and responsibility for the management of information and information systems across the organization.

5. Business Enablement

Drive excellence in security by aligning with business goals and fostering partnerships that support innovation and growth.

6. Stakeholder Collaboration

Encourage active collaboration across internal and external stakeholders to enhance our collective security posture.

7. Security Culture

Cultivate awareness and continuously advocate for security as a shared responsibility throughout Publicis Groupe.

Security Objectives

1. Safeguard Business Information

Protect information necessary to operate effectively and achieve strategic objectives.

2. Protect Client Trust

Secure the data entrusted to us by clients and meet their evolving security expectations.

3. Ensure Compliance

Adhere to applicable laws, regulations, and contractual obligations concerning Information Security.

4. Manage Risk

Identify, evaluate, and mitigate internal and third-party security risks to maintain them within acceptable thresholds.

5. Enable Secure Innovation

Implement security by design into new technologies and business initiatives.

6. Ensure Resilience & Continuity

Maintain the ability to detect, respond to, and recover from incidents with minimal disruption to critical business operations.

Security Framework

Publicis Groupe uses ISO 27001 standards as the foundation for its global security program. Certain critical business areas are in scope of ISO 27001 certification and regularly audited.

HOW?

Global Security Office (GSO)

The Global Security Office (GSO) is a dedicated security organization tasked with executing the Information Security program's charter.

The GSO comprises over 150 security professionals who possess industry-recognized certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Security Auditor (CISA), Certified Ethical Hacker (CEH) among others.

As a shared services organization for all Publicis Groupe agencies worldwide, the GSO provides security services across all geographic regions. The GSO's vision, mission, and services are detailed as follows:

Vision

Create a competitive advantage for Publicis Groupe by transparently promoting security through collaboration.

Mission

- Positioning the GSO as subject-matter experts within Publicis Groupe and the Information Security industry.
- Working with agencies, clients, and other stakeholders to understand their business and security needs, expectations and priorities.
- Simplifying interactions between agencies, teams, and the GSO.
- Promoting and spreading security awareness continuously.

Services

The GSO delivers a range of services to Publicis Groupe Business Units aimed at implementing the Groupe's Information Security program charter.

- Information Security policy lifecycle management

- Security training and awareness
- Security framework (e.g., ISO 27001, SOC 2, PCI-DSS, TISAX) adoption, implementation and certifications
- Client security requirements support
- Business continuity framework (e.g., ISO 22301) adoption, implementation and certification
- Security risk management, including supplier security risk assessment
- Security testing, e.g., vulnerability scanning, penetration testing, etc.
- Security architecture review and guidance
- Security incident management
- Security operations

The Groupe's 24/7 Security Operations Center (SOC) continuously monitors, analyzes and responds to security events across the entire network, infrastructure and applications.

The GSO collaborates with the Groupe's Global Data Privacy Office (GDPO), Procurement, and Legal departments to understand and comply with data privacy-related legal, contractual, and regulatory requirements.

The GSO collaborates with the Groupe Risk Management and Insurance teams on the annual program for cybersecurity risk evaluation.

Security Governance

The GSO, led by the CISO, reports to the CEO of Re:Sources, Publicis Groupe's Shared Services Organization. Information Security program is overseen by the Secretary General who provides strategic guidance. The Audit and Financial Risks Committee is regularly updated of the Information Security strategy.

Security Policies

Publicis Groupe uses a layered security approach with industry-standard administrative, physical, and technical controls at organizational, system, and network levels.

At the highest level of this layer are the Information Security policies that have been developed to align with the industry recognized ISO 27001 framework.

These security policies guide management and support Information Security goals. They establish minimum standards to maintain and enhance security at Publicis Groupe.

Below is a summary of all policy documents available to employees, updated regularly to meet evolving business needs.

POLICY NAME	PURPOSE
Information Security Policy	Provides direction on principles, objectives, controls and overall governance of Information Security
Access Control Policy	Provides direction on controlling access to Groupe information and facilities
Network Security Policy	Provides direction on protecting and securing the Groupe network
Cloud Security Policy	Provides direction on securely hosting or using internal or external cloud solutions
Acceptable Use Policy	Provides direction on the acceptable use of information assets and encourages responsible behavior for safeguarding information
Mobile Device Policy	Provides direction on the secure usage of mobile devices and Bring Your Own Device (BYOD) arrangements
Incident Response Policy	Provides direction on how to handle a breach of sensitive information in accordance with international and local laws and regulations



Publicis Groupe employees, freelancers, and contractors are required to read, understand, and comply with the Information Security policy requirements.

Any violation of a security policy is considered a security breach. The consequences of a confirmed breach may include disciplinary action, up to and including termination of employment or contract, as well as potential civil or criminal action or prosecution for each offense.

Security Awareness Program

Publicis Groupe’s security awareness program aims to create a security-aware workforce and reduce cybersecurity risks. All employees must complete the mandatory annual training as part of Publicis Groupe’s commitment to Information Security and data protection. The program uses micro-learning experiences and tailored content for high-risk groups to promote security-conscious behaviors. The security awareness program aims to:

- Raise awareness of responsibilities for protecting client and Publicis Groupe information per the security policies.
- Educate on security best practices and standards.
- Train to recognize and report incidents impacting client or Publicis Groupe information.

Security awareness material is created and distributed through various communication channels, both internal and external. These include online and offline training sessions, awareness campaigns, security articles, videos, announcements, and collaboration channels. These methods emphasize the importance of maintaining good Information Security practices through consistent messaging and informing individuals on how to safeguard client and Groupe information.

The effectiveness of the security awareness program is evaluated using phishing tests, which simulate real-world malicious email messages and are conducted regularly throughout the year.

ISO 27001 Certification & External Verification

Publicis Groupe’s security program aligns with ISO 27001 standards.

Also, the Groupe’s Information Security Management System (ISMS) is audited annually by external auditors.

Security Incident Response

Publicis Groupe has a strong Incident Management program. Employees, freelancers, and contractors can report security events via Helpdesk or email to the GSO security incident response team at reportincident@publicisgroupe.com.

Depending on severity, the response bridge is activated, and key members address the issue. Stakeholders are informed of actions taken, and incidents are closed with a report and recommendations.

The agency contact, supported by the Incident Response Team, communicates incidents to clients with input from legal and privacy teams.

Data Centers, Servers and Cloud

Publicis Groupe uses reputable data center providers to host its information, which are regularly assessed by independent third parties and hold certifications like ISO 27001, SOC 1, and SOC 2.

Publicis Groupe has also advanced in its cloud journey, with many critical applications now benefiting from the scalability, security, and agility of cloud architecture.

To safeguard our information assets in the cloud, GSO oversees Cloud Security Posture Management Systems, including CNAPP (Cloud Native Application Platform Protection) and SSPM (SaaS Security Posture Management). These systems monitor all cloud services within the Group from the perspectives of security configuration, adherence to industry best practices, and policy compliance.

Business Continuity and Disaster Recovery

Publicis Groupe has established comprehensive business continuity and disaster recovery plans.

The strategy for business continuity planning includes enabling a mobile workforce and promoting teleworking. This is achieved by providing People with mobile computing and connectivity capabilities, allowing them to work from remote locations, thereby reducing reliance on Publicis Groupe facilities for business operations.

WHO?

Country and Business Unit CEO's, CFO's, and Head of Technology/Engineering, SSC, Global Security Office and Re:Sources IT.

Policy available to the public on the Groupe website.