II. THE PUBLICIS WAY TO WORK TOGETHER

6. INFORMATION *SECURITY*

WHY?

Within Publicis Groupe, safeguarding the information we hold both for ourselves and our clients is **everyone's responsibility**. There is a formal information security program in place to address the security requirements of Publicis Groupe as well as its clients.

FOR WHOM?

Publicis Groupe's IT Security Policy applies to all employees, temporary workers, interns, and other workers at Publicis Groupe, its agencies, business units and shared solution centers, and authorized third parties (freelancers, contractors, consultants, suppliers, etc.) collectively called 'People' in this document. Publicis Groupe and its agencies (including business units and shared solution centers) are collectively called 'Groupe' in this document.

WHAT?

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

Security Principles

1. Respect for the legitimate rights and interests of others (ethical use of security).
2. Transparency in achieving security objectives.
3. Proportionality of security controls to assessed or perceived risks.
4. Ownership and accountability of information and information systems.
5. Excellence through partnership and business enablement.
6. Collaboration among business and external stakeholders.
7. Awareness and promotion of security.

Security Objectives

1. Protect the information necessary to run the business and meet our strategic goals and objectives.
2. Protect the information our clients entrust us with and address their security requirements.
3. Comply with applicable laws, regulations and contractual requirements.
4. Manage security risks to acceptable levels.

Security Framework

Publicis Groupe has adopted industry-recognized ISO 27 001 information security standard as baseline on which the global security program has been built. Certain critical business areas are formally ISO 27 001 certified and undergo periodic internal and external audits.

HOW?

Global Security Office (GSO)

There is a dedicated security organization 'Global Security Office' (also known as the GSO) that is responsible for carrying out the charter of the program. This organization consists of 100+ security professionals who hold industry recognized certifications such as CISSP, CISM, CISA, etc., among others. The GSO is a common shared services organization for all Publicis Groupe agencies globally and has presence in all geographic regions, namely, the Americas, Europe and Asia Pacific. The GSO's vision, mission and Services are as follows:

Vision

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

Mission

- Establishing the GSO as subject matter experts not only in the Groupe, but also in the information security industry.
- Partnering with agencies, clients and other stakeholders to truly understand their business and security needs, expectations and priorities.
- Simplifying the way agencies and teams interact with the GSO.
- Collaborating and spreading security awareness at all times.

Services

The GSO provides the following services to Publicis Groupe business units to carry out the information security program charter of the Groupe:

- Information security policy lifecycle management.
- Security training and awareness.
- Security frameworks (e.g, ISO 27001) adoption, implementation and certifications.
- Client security requirements support.
- Business continuity framework (e.g, ISO 22301) adoption, implementation and certifications.
- Security risk management, including third-party risks.
- Security testing e.g, vulnerability scanning, penetration testing, etc.
- Security architecture review and guidance.
- Security incident management.
- Security operations.

The Groupe also has a **24/7 dedicated Security Operations Center** (SOC) under the IT organization that monitors security events for any potential adverse impact on the Groupe network or infrastructure.

The GSO works closely with the Groupe's Global Data Privacy Office (GDPO) and Legal department to understand and comply with the applicable data privacy-related legal, contractual and regulatory requirements of the world. Thanks to the close partnership between the GSO and GDPO, Publicis Groupe is well prepared to address the requirements regulations such as the European General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

Security Governance

The GSO has a strong leadership that reports up to the management of the company. The team is led by the Office of the CISO (Chief Information Technology Security Officer) and reports directly to the CEO of Re:Sources, Publicis Groupe's Shared Services Organization. Information Security is supervised by the Publicis Groupe leadership, i.e. the Secretary General, member of the Management Board (Directoire) and the CEO Shared Platforms, member of the Management Committee, who provide strategic guidance and direction to the information security program and also monitor its effectiveness.
Executive reports about the overall health of information security program and maturity are provided by the GSO to the Supervisory Board Strategy & Risks Committee quarterly.

Security Policies

Publicis Groupe follows a 'layered' approach model for implementing security that consists of a combination of industry-recognized administrative, physical and technical security controls also called "technical and organizational measures" at the organization, system and network layers.
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 provide management direction and support for information security objectives. They also define minimum standards that must be met to maintain and improve information security at Publicis Groupe. Following is the summary of all information security policy documents that are available to all employees, and are updated on a regular basis to meet the ever-changing business requirements.

Publicis employees, freelancers and contractors must read, understand, and adhere to the information security policy requirements.

Violation of any security policy is a security breach. Consequences of a confirmed breach may include disciplinary action up to and including termination of employment or contract, as well as civil or criminal action, or prosecution for each offense.

Security Awareness Program

The Groupe security awareness program has been developed to create a security-conscious workforce and minimize cyber security risks for the Groupe. Every employee is required to take the mandatory security awareness training annually as part of Publicis Groupe's commitment to information security and data protection. The strategy is to provide human-friendly micro-learning **(series of short and focused e-learning)** experiences to People and tailored content to higher risk groups to drive security conscious behaviors. The security awareness program aims to:

- Create awareness of people's responsibilities regarding the protection of client and Groupe information, as defined in the Groupe security policies.
- Educate people on security best practices, applicable security standards, contractual and legal security requirements.
- Train people on recognizing suspected or actual incidents that impact client or Groupe information and how to report these incidents.

Security awareness material is created and disseminated via multiple communication channels (internal and external) such as: online and offline training and awareness campaigns, including security articles, posters, bespoke videos, announcements, collaboration channels, etc. These methods support and reinforce the importance of good information security practices through consistent messaging and engaging people on how they can help protect client and Groupe information. The effectiveness of security awareness program is measured through phishing tests (emails simulating real-world malicious messages), which are conducted regularly all through the year.

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

ISO 27001 Certification & External Verification

Publicis Groupe's security program and policies are designed to align with the requirements of ISO 27001 global information security standard.

Critical business areas of the company in certain offices (e.g, backend IT shared services infrastructure, Epsilon business, etc.) are formally ISO 27001 certified and undergo periodic external audits with the certifying organizations.

The established Information Security Management System under the scope of ISO 27001 certification is audited annually by the external certification body auditors. Vulnerability scans are performed on Groupe network perimeter on fortnightly basis by the security organization of the company. Identified vulnerabilities are remediated according to their priority. There is also an independent test of our network perimeter that is performed by a third party annually.

Security Incident Response

Publicis Groupe has a robust Incident management program. Publicis employees, freelancers and contractors can report security incidents through the Helpdesk, or by sending an email to the GSO incident response team. Based on the severity of the incident, the incident response bridge is activated and select incident response members convene to address the situation. Pertinent stakeholders are informed of the incident and actions taken. Incidents are closed with the investigation report and any highlighted learnings in order to reduce likelihood and impact of future incidents. The agency contact is responsible for communicating the security incidents to clients with support from the Incident response team and with input from relevant legal and privacy teams.

Data Centers, Servers and Cloud

Publicis Groupe avails services from reputed datacenter providers to host its information. These datacenter providers undergo regular independent assessment from accredited third parties and maintain industry certifications such as ISO 27001, SOC 1, SOC 2, etc., to name a few. Servers and other technical infrastructure are located in locked cages within these datacenters. Layered security model is implemented to control physical and logical access to these datacenters and servers. Servers are hardened as per industry best practices and continuously monitored to ensure confidentiality, integrity and availability of information. Over the last few years, Publicis Groupe made significant steps on its cloud journey. Many critical applications and services today are cloud-based and benefit from the scalability, security and agility of the cloud architecture.

To ensure security of our information assets in the clouds, GSO manages Cloud Security Posture Management Systems such as CNAPP (Cloud Native Application Platform Protection) and SSPM (SaaS Security Posture Management), these systems do monitor all cloud services in the Groupe from a security configure, industry best practices and policy compliance standpoint.

Business Continuity and Disaster Recovery

Publicis Groupe has comprehensive business continuity and disaster recovery plans in place. The strategy adopted for business continuity planning includes mobile workforce enablement and teleworking. This is implemented by providing mobile computing and connectivity capabilities to People that enables them to work from 'remote' locations, thus eliminating the dependencies upon the Publicis Groupe facilities to continue business operations. Project or operations-specific recovery plans, referred to as the Business Continuity Recovery Plans (BCRP), for dealing with longer-term outages and disasters, specific to a critical project, client-work, business operations or a function, are created on client or project-need basis.

WHO?

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