OMNICOM

CORE IT GOVERNANCE POLICIES

OMNICOM
CORE IT GOVERNANCE
POLICIES

UPDATED NOV. 2025

CONFIDENTIAL —
NOT FOR EXTERNAL
DISTRIBUTION

ACCEPTABLE USE GOVERNANCE POLICY

Purpose & Scope

The policy aims to protect Omnicom and client information by setting standards for information security, proper use of IT systems, and compliance with legal obligations.

Applies to all employees, contractors, affiliates, and anyone accessing Omnicom systems or data worldwide, subject to local laws.

Core Principles

Professionalism & Integrity: All users must act responsibly, honestly, and professionally when using company technology and data.

Security: Devices and systems must be kept secure (passwords, encryption, locked when idle). Unauthorized access is strictly prohibited.

Clear Desk/Clear Screen: Confidential information must be protected from unauthorized viewing, both physically and digitally.

Annual Training: Mandatory for all staff, covering ethics, security, privacy, and compliance topics.

Key Obligations

Physical Asset Protection: Devices must be secured at all times; loss or theft must be reported immediately.

Authentication: Passwords must meet company standards, be kept confidential, and changed regularly.

Removable Media: Use is restricted unless specific approval is received by IT security. Exceptions can be requested via ServiceNow.

Information Storage: Only approved Omnicom IT storage solutions may be used; personal cloud services are prohibited for work data.

Digital Transfers: Use only approved methods; encryption required for sensitive data; peer-to-peer file sharing is banned.

Email & Communications: Use only company accounts for business; maintain professionalism; avoid sending confidential info via personal accounts.

Disposal: Securely destroy physical and electronic assets per company policy.

Travel: Take precautions with devices when traveling; avoid public/shared computers.

Prohibited Activities: Includes accessing or sharing offensive, illegal, or unauthorized materials, and unauthorized disclosure of confidential information.

OMNICOM

Personal Devices: Permitted for work if enrolled in our Mobile Application Management (MAM) policy.

MAM Software: Required for all devices accessing company systems; controls access to Omnicom data via mobile device.

Costs & Support: Employees are responsible for costs and insurance of personal devices; company provides limited support.

Monitoring: For corporate issued systems, we may monitor usage, access and communications for security and compliance reasons.

Note for users with MAM Software on personal devices: We will not have access to any of your personal data, information, or apps in any form at any time.

AI & Automation: Use of AI and automation must comply with ethical principles, data protection, and company policies. Generative AI requires human oversight and compliance with Omnicom's AI Council guidelines.

Incident Reporting: Security incidents and data breaches must be reported immediately via designated channels. Failure to report may result in disciplinary action. To report security incidents:

- **Omnicom employees:**
  - Contact Corporate Security at infosec@omnicomgroup.com;
  - Open a Paige ticket via "I think I may have a security/privacy issue";
  - Email soc@omnicomsecurityservices.com; or
  - Call the Service Desk at 1-800-MY-PAIGE.
- **Interpublic Employees:** Email: IncidentResponse@interpublic.com
- **Note:** Common reporting channels will be available in the near future.

Data Governance Overview

Data Governance is the disciplined management and protection of our organization's data, guided by policies, procedures, and standards for collecting, storing, using, and safeguarding information. Our policies and standards for Global Data Protection and Privacy, Information Governance and storage standards, Information Classification, Data Retention and Records Management with its Records Retention Schedule, and the detailed Information Handling Standard protect company assets and strengthen client confidence in our security and privacy. A key overall success factor is clear Data Ownership in the business, close to the data and the business requirements.

Data Governance Engagement Model & Framework:

OMNICOM

Spend Governance Overview

Agencies submit spend requests through our centralized ServiceNow platform. Each request must be accompanied by justification, supporting documentation, alignment with the approved budget, and require various levels of CFO approval based upon the amount of spend requested.

Category: Artificial Intelligence, Cloud Computing, Collaboration, Communications, Connectivity (Circuits), Cybersecurity, Data Storage, Endpoints, Infrastructure, Messaging, Monitoring, Network Security, Software Development, Systems and Platforms.

Subcategory: Consulting, License (Software), Maintenance Agreement, Product (Hardware), Professional Services.

Performing Risk Assessments for Any Software: Requires a formal risk assessment process before deploying or integrating new software. This ensures that potential security, privacy, and operational risks are identified and mitigated.

Working with Approved Vendors: Mandates the use of vendors who have been vetted and approved in accordance with Omnicom's risk and compliance standards and ensures that partners meet Omnicom's governance requirements.

Enterprise Agreements: Working within our single negotiated umbrella agreement that provides standard products, services, or rights to multiple Omnicom entities.

Password Policy

As legacy Interpublic employees prepare to migrate to @omc.com during the course of 2026, additional IT policy updates will take effect—most notably, alignment with Omnicom's password policy.

Password guidelines and best practices:

- Do not recycle your password for different Omnicom accounts or systems
- Passwords cannot be any of your last 8 password(s)
- Passwords must be changed every 90 days or sooner
- Passwords cannot contain any parts of your username
- Do not share your passwords with anyone, including managers or IT support staff
- Store your passwords securely—do not write them down or save them on unencrypted devices, in contacts, calendar entries, Word files, etc.

New passwords must meet the following criteria:

- Be at least 15 characters long
- Contain at least one uppercase letter (A through Z)
- Contain at least one lowercase letter (a through z)
- Contain at least one number
- Contain at least one distinctive character (# % $ @)
- Must not contain any personal or common information, such as names, dates or phone numbers