INFORMATION SECURITY POLICY

The purpose of this policy is to describe the general security principles defined by MEDIACROSS in order to develop an efficient and secure Information Security Management System (ISMS) in accordance with ISO 27001.

For MEDIACROSS, information security has the primary objective of protecting data and information, as well as the technological, physical, logical, and organizational structures responsible for their management.
This means achieving and maintaining a secure information management system by ensuring the following properties:

1. Confidentiality: ensuring that information is accessible only to those who are duly authorized to access it;
2. Integrity: safeguarding the consistency of information against unauthorized changes;
3. Availability: ensuring that authorized users have access to information and related assets when required;
4. Control: ensuring that information management systems are subject to systematic and effective controls.

Within the scope of MEDIACROSS activities, information security covers the technological infrastructure, organizational structure, operational procedures, and activities carried out to protect information assets.
The objectives of information security are pursued by implementing organizational and technical measures designed to protect information and reduce the risks associated with its potential compromise.

For this purpose, MEDIACROSS has developed a secure information management system in compliance with the requirements of ISO 27001:2022 and applicable laws, as a means to manage information security in the course of its operations.

The information security policy applies to all internal staff as well as third parties (e.g., service providers, maintenance, support, etc.) involved in the management of information and to all processes and resources involved in the design, implementation, delivery, and continuous provision of services.

MEDIACROSS reviews this policy at least annually, taking into account the operating context, stakeholders, opportunities, and risks that could impact its Information Security Management System.

The policy represents the organization’s commitment to clients and third parties to

guarantee the security of information, through appropriate physical, logical, and organizational security measures.

Principles of MEDIACROSS information security policy:
- Guarantee logical access controls (see attached “Access Control Policy”);
- Ensure data classification and secure treatment (see attached “Data Classification Policy”);
- Ensure safe physical access and secure work environments;
- Adopt organizational and technical measures such as:
  1) clear desk and clear screen policies;
  2) use of strong passwords;
  3) clean and regularly maintained premises;
  4) regulated use of mobile devices and remote working;
  5) restrictions on software installation and usage;
  6) establish and perform backups at regular intervals;
  7) secure transfer of information;
  8) malware protection;
  9) identification, monitoring, and management of technical vulnerabilities;
  10) cryptographic controls, where necessary;
  11) secure communications;
  12) compliance with applicable privacy and data protection laws;
  13) regulated supplier relationships in accordance with ISO 27001.

Scope of application of this policy (activities carried out by MEDIACROSS):
- Design, development, and support of software;
- SaaS cloud services.

Firenze, 15/05/2024