



Information Security Policy
Version 2.0

15 March 2025

Information Security Policy

The current era is often referred to as the “information age”. We have seen a massive change in the way humans generate, store and exchange information. It has also profoundly altered the terms by which we interact with each other, not just as individuals, but also within and between institutions, societies and nations. We have accrued great benefits from this new era, but it brings with it profound challenges in the areas of security and privacy, which have been reflected in the growth of legislation around the globe concerning the holding of information.

Moptil is required to maintain long-term relationships with its customers and to provide excellent services, striving to successfully address the problems and needs of service providers worldwide for automated pricing and provisioning through innovation and advanced technology.

Moptil has an ethical, legal and professional duty to ensure that the information it holds conforms to the principles of confidentiality, integrity and availability. We must ensure that the information we hold or are responsible for is safeguarded where necessary against inappropriate disclosure; is accurate, timely and attributable and is available to those who should be able to access it.

In order to serve the above, Moptil recognizes the Information Security threats that are generated and traded within its activities and has all the resources required to protect its information.

This policy is applicable to, and will be communicated to, all staff and third parties who interact with information held by Moptil and the information systems used to store and process it. This includes, but is not limited to, any systems or data attached to Moptil’s data or networks, systems managed by Moptil, mobile devices used to connect to Moptil networks or hold Moptil data, data over which Moptil holds the intellectual property rights, data over which Moptil is the data controller or data processor, communications sent to or from Moptil.

The **commitment** to Information Security and the avoidance of incidents that may affect the company, are implemented through the following steps:

- 🚩 Protection of the resources and the information handled by the company from any threat, internal or external, deliberate or accidental,
- 🚩 Systematic assessment and evaluation of information security risks, aiming to their sound and timely treatment / management,

- ✚ Secure application, systems and services development and maintenance processes,
- ✚ Data archiving, viruses and outside intrusion minimization, access control systems, keeping records of all security incidents and managing unexpected developments,
- ✚ Keeping management and personnel informed regarding information security,
- ✚ Control of exchanged data and information in transit,
- ✚ Protection of the interests of the company and of those who do business with it and trust it,
- ✚ Immediate and effective handling of security incidents and breaches,
- ✚ Encouraging internal communication on Information Security issues,
- ✚ Commitment to the faithful implementation of the Security Policies and all applicable national and EU legislation.

Moptil is committed to continuous improvement efforts of its information protection so that it can offer high levels of security to those who do business / deal with the company.

Moptil has developed and implements an Information Security and Privacy Management System that conforms to ISO 27001:2022 and ISO 27701:2019 standards, which includes Information Security Policies, on the topics of Acceptable Use, Physical Security, Access Control, Remote Access Control, Security Incident Management, Supplier Security, Removable Media, Malware Protection, Cryptography and other.

Moptil's Information Security Policy, and all individual Policies, are inextricably linked to the company's objectives and vision, are appropriate to the company and ensure its position on the market in which it operates.

Information security policies shall be reviewed at least once a year and whenever significant changes take place to ensure their relevance, adequacy and effectiveness.

Commitment

The following **information security principles** provide governance for the security and management of information at Moptil:

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with relevant legislative, regulatory and contractual requirements and the company's Information Security Policies.
2. Staff must ensure the classification of information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
3. All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. On this basis, access to information will be on the basis of least privilege and need to know.
5. Information will be protected against unauthorized access and processing in accordance with its classification level.
6. Breaches of this policy must be reported to the Information Security Manager.
7. Information security provision and the policies that guide it will be regularly reviewed, including the use of annual internal audits and penetration testing.

Moptil's Information Security Policy provide the framework by which we take account of these principles. Its primary purpose is to enable all Moptil staff to understand both their legal and ethical responsibilities concerning information, and empower them to collect, use, store and distribute it in appropriate ways.

This policy is the cornerstone of Moptil on-going commitment to the implementation and maintenance of the highest standards of security across the company and to the enhancement and clarification of our information security procedures. It has my full support and I expect all Moptil staff to share this commitment, read the Information Security Policy and abide by it in the course of their work.

Michael Kokkinos

CEO