INFORMATION SECURITY POLICY IN THE RELATIONSHIP WITH SUPPLIERS

▪ Knowledge of the Policy

This Policy must be made available to all suppliers with access to information assets and/or DUO Capital's facilities, during the contractual relationship, as an addendum to the service provision contract or, in cases previously contracted, by sending a circular, e-mail or other documented form.

▪ Documented Agreement

It must be established in a contract, or at least in a documented agreement, with Suppliers not certified in ISO/IEC 27001 which information security rules must be complied with, namely:

- Service Level Agreement (SLA) assumed;
- Training and awareness of its employees, in order to ensure a practice in accordance with the legal rules of information security and protection of personal data;
- Communicating to your employees the requirements agreed in the contract, in order to ensure their compliance;
- Report information security incidents immediately, whenever they occur.

▪ Confidentiality or Non-Disclosure Statement

Suppliers involved in a process of acquisition of products and/or services, in which they need to have access to sensitive information, must sign a **Declaration of Confidentiality or Non-Disclosure**, which may or may not be included in the contract for the acquisition of products and/or services.

Confidentiality or non-disclosure agreements must be drafted in a manner that protects confidential information, in compliance with applicable law.

These agreements should consider the following points:

- Definition of the information to be protected (confidential information and personal data);
- Expected duration of the agreement, including deadlines for maintaining confidentiality;
- Actions required when the agreement ends, including conditions for the return or destruction of information;
- Responsibilities to prevent unauthorized disclosure of information;
- Ownership of information, intellectual property and protection of commercial information;
- The permitted use of confidential information and the copyright to use the information;
- The right to audit activities involving confidential information;
- Process for notifying and reporting unauthorized disclosure or leakage of confidential information;
- Actions in the event of a breach of agreement.

- Information Security Requirements by Supplier

Whenever there is a need for the existence of a contract or equivalent, these will include the obligation to comply with requirements of confidentiality of information and protection of personal data, according to the previous points and respecting, at least, the following:

Supplier Types	Information Security Requirements	Information assets accessed	Classification of information
Services Communications	Service Level (SLA) Rate availability	Network/internet	Confidential
IT Maintenance Services	Service Level (SLA) Confidentiality agreement	Hardware	Confidential
Support Services (Service Desk)	Service Level (SLA) Confidentiality agreement	Software	Confidential
Cloud Services	Service Level (SLA) Rate availability Contract as a subcontractor ISO 27001 Certification	Software & Files	Confidential
Cleaning services	Confidentiality Agreement Training/awareness-raising List of persons authorised to access the facility	Facilities	Internal
Vending services	Confidentiality Agreement	Facilities	Internal
Consulting Services	Service Contract Confidentiality Agreement	Sensitive organization documents	Confidential
Temporary employment	Service Contract Confidentiality Agreement	Documents	Confidential

- Access to DUO Capital's Facilities

Access to the premises must comply with the following rules:

- Suppliers accessing the premises must be accompanied at all times;

- Access to the *wireless* network is only allowed for the guest network, and the access password for the guest network is provided;
- The use of portable disks or PEN within the premises, by service providers, is not allowed unless explicitly authorized by the *Management Team.*

List of Suppliers

Suppliers with access to DUO Capital's information assets and/or facilities are duly identified in the **Suppliers List**.

Failure to comply with the Policy

Non-conformities or violations of security policies or procedures are subject to penalty and/or breach of contract.