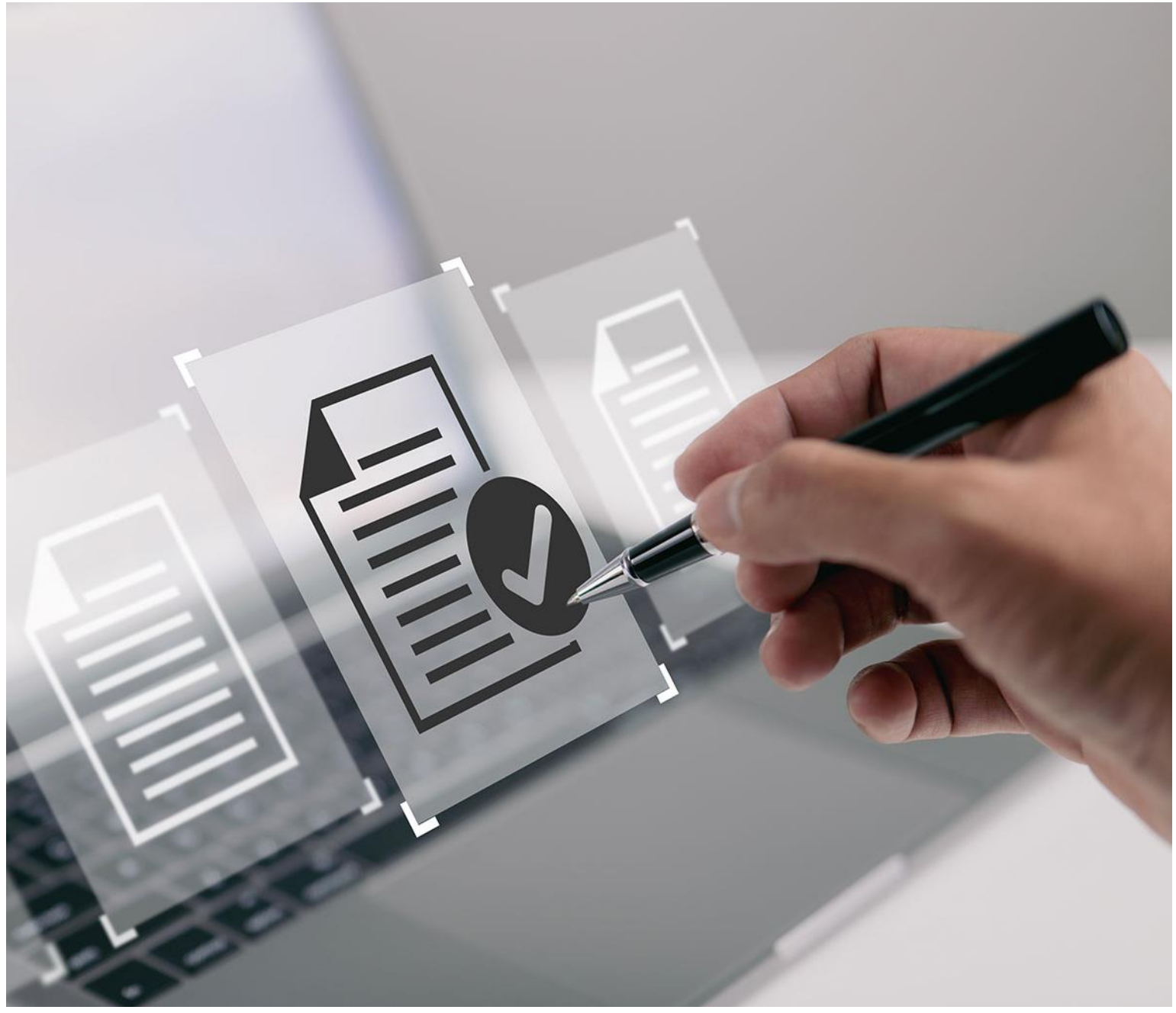
MakoLab S.A.

Supplier Relations Management Policy

23 MAY 2023

Document extract



MakoLab | MakoLab S.A.
Supplier Relations Management Policy

Document extract

Information may only be conveyed to external entities by a person authorised to do so and within an approved scope, which arises from the purpose of conveying the information. The Asset Owner is responsible for authorising the person and approving the scope in accordance with the principles adopted for classifying information and proceeding with it.

Information may be conveyed to external entities for a purpose other than compliance with the applicable legal requirements once a contract has been signed with the entity in question.

Under the contracts binding on them, companies and people collaborating with MakoLab S.A., hereinafter referred to as 'Associates', are obliged to comply with legal standards and regulations concerning security. Associates must obligate their members of staff and associates to comply with the requirements and regulations in this respect.

In terms of information security, monitoring the activities of Associates covers the same requirements as for the verification of the Staff [of MakoLab S.A.]. Any and every permission and right to access is issued in accordance with POL#016 Access Control Policy EN Rev.D. Associates must confirm the receipt and return of company equipment. In justified instances, and after consulting the Proxy for the Information Security Management System, the Member of Staff responsible for coordinating a given collaboration decides whether or not the Associate in question can participate in training.

The Proxy for the Information Security Management System stipulates the requirements for monitoring companies and associates. Sanctions in accordance with the applicable law will be imposed on Associates who violate the rules for security.

Contracts with suppliers of services should be documented and contain the necessary requirements in respect of information security.

The management of changes to services provided should take into account the criticality of the systems and business process they are related to and should include a risk assessment.

Document extract

Each Member of Staff coordinating a collaboration with an Associate is responsible for ensuring the requisite protection of any information exchanged and for supervising the activities of external parties throughout the duration of their contracts.

The forms appropriate to the type of collaboration and its scope are completed in conjunction with the Supplier and held with the documentation for the selection of that Supplier:

- FOR#001 General Terms and Conditions for Collaboration, irrespective of the type of collaboration with the Supplier
- POL#015#FOR#002 Information Classification EN Rev.E, irrespective of the type of collaboration with the Supplier
- POL#015#FOR#003 Supplier Evaluation Spreadsheet EN Rev.E, for IT service Suppliers, such as subcontractors, for example
- POL#015#FOR#004 Internet Service Providers EN Rev.E, for ISPs
- POL#015#FOR#005 Hardware Suppliers EN Rev.E, for hardware Suppliers
- POL#015#FOR#006 Cloud Service Providers EN Rev.E, for Suppliers of Cloud services
- POL#015#FOR#007 Verification Questionnaire for Processing Entities EN Rev.E, irrespective of the type of collaboration with the Supplier; this requirement results from POL#018 Personal Data Protection Policy EN Rev.C

Purpose and scope

Purpose and scope

The purpose of this document is to ensure the appropriate information security protection between MakoLab S.A., hereinafter referred to as ‘the Company’ and contractors/suppliers, hereinafter referred to as Suppliers, in respect of programming and information services provided to the Company.

Terms and definitions

The terms and definitions used in this document are taken from
Słownik pojęć w Zintegrowanym Systemie Zarządzania
- Dictionary of terms constituting part of the Integrated Management System.

MakoLab S.A. Supplier Relations Management Policy

General principles

Exchanging information with external entities

Information may only be conveyed to external entities by a person authorised to do so and within an approved scope, which arises from the purpose of conveying the information. The Asset Owner is responsible for authorising the person and approving the scope as part of their work and in accordance with the principles adopted for classifying information and proceeding with it. In particular, the authorisation specifies the entities and representatives thereof to whom information may be conveyed and the scope of the information which it is permissible to convey.

Information may be conveyed to external entities for a purpose other than compliance with the applicable legal requirements once a contract has been concluded with the entity in question. The contract should:

1. stipulate the accepted purpose for processing the information conveyed;
2. stipulate the accepted period during which the entity will process the information conveyed;
3. stipulate the entity's obligation to maintain the secrecy of the information conveyed, if applicable;
4. set out instructions on the basic requirements for securing the information conveyed;
5. stipulate the method of proceeding if there should be a breach of security in respect of the information processed by the entity and conveyed by the Company. The method must include, at the very least, notifying the Company of the occurrence of an event;
6. stipulate the method of proceeding with information conveyed to, or obtained by, the entity when the information is indispensable to the entity for the performance of activities pursuant to the contract. The method must cover conveying the original documents to the Company and destroying every copy held by the entity or, should it be impossible to convey the original documents, such as electronic documents, for instance, then the destruction of all the documents and information in question and the confirmation of the fact by way of a formal record;
7. stipulate the principles for the exchange of information between the parties, in accordance with this policy.

General principles

Exchanging information with external entities

When legally protected information constituting a business or telecommunications secret is conveyed to external entities by means of removable media, hard copies or digital copies, this must occur in a regulated manner.

Providing access to legally protected information, particularly personal data, should be carried out as stipulated in the applicable laws and within the limits set out therein.

General principles

Associates

Companies and people collaborating with MakoLab, hereinafter referred to as ‘Associates’, are subject to monitoring in respect of compliance with the security procedures in place at the Company. Under the contracts binding on them, Associates are informed of their obligation to comply with legal standards and regulations concerning security.

The contracts and additional declarations contain provisions in respect of adhering to the security requirements and regulations. The contracts also contains restrictions to which the Associate will be subject should they violate the aforementioned regulations during the legal relationship between the parties.

In accordance with the applicable law, Associates will be notified when a verification process is to be carried out for the purpose of checking whether they are meeting the security requirements. They must give the appropriate consent to the verification.

The scope of the obligations set out in the contract in respect of security depends on the type of collaboration and its duration. It also depends on the security risks connected with an Associate’s given activity and, in addition, it accords with the business priorities determined by the Company.

Care should be taken to ensure that, following the termination of a contract with an Associate, the Company incurs no damages as regards loss of information or company equipment or the disclosure of any third party’s confidential data.

General principles

Materials and measures used for drawing up and concluding a contract

The activities of the Company's Associates are regulated by an appropriate contract, which stipulates any and every necessary permission and right to access. Associates must obligate their members of staff and associates to comply with the requirements and regulations in respect of security.

In accordance with the regulations, Associates who have access to information protected by law are also obliged to maintain its confidentiality.

The contract and any declarations from Associates whereby they take on obligations in respect of security contain a provision concerning confidentiality and maintaining secrecy. The provision also related to after the contract is terminated.

The contract stipulates the sanctions, which is to say, contractual penalties, imposed on an Associate if they violate the security requirements. As soon as an Associate starts work, the Member of Staff responsible for coordinating the collaboration with them ensures that the Associate is fully informed as to the obligations incumbent on them and provides appropriate monitoring.

In terms of information security, monitoring the activities of Associates covers the same requirements as for the verification of the Company's Staff.

General principles

Materials and measures used for drawing up and concluding a contract

The forms appropriate to the type of collaboration and its scope are completed in conjunction with the Supplier and held with the documentation for the selection of the Supplier:

- FOR#001 General Terms and Conditions for Collaboration, irrespective of the type of collaboration with the Supplier
- POL#015#FOR#002 Information Classification EN Rev.E, irrespective of the type of collaboration with the Supplier
- POL#015#FOR#003 Supplier Evaluation Spreadsheet EN Rev.E, for IT service Suppliers, such as subcontractors, for example
- POL#015#FOR#004 Internet Service Providers EN Rev.E, for ISPs
- POL#015#FOR#005 Hardware Suppliers EN Rev.E, for hardware Suppliers
- POL#015#FOR#006 Cloud Service Providers EN Rev.E, for Suppliers of Cloud services
- POL#015#FOR#007 Verification Questionnaire for Processing Entities EN Rev.E, irrespective of the type of collaboration with the Supplier; this requirement results from POL#018 Personal Data Protection Policy EN Rev.C

General principles

Materials and measures used during collaboration

1. Any and every permission and right to access is issued in accordance with POL#016 Access Control Policy EN Rev.D.
2. Company equipment issued to an Associate for the performance of the tasks assigned to them. The provision and return of equipment and other company property is documented by the Company's appropriate organisation unit, namely, the IT Team. Associates must confirm the receipt and return of company equipment.
3. In justified instances, and in the light of the type of activity and level of security, Associates employed by the Company should participate in training which will increase their sense of awareness regarding matters of security. The decision as to an Associate's participation in training is taken by the Member of Staff responsible for coordinating the collaboration, after consultation with the Proxy for the Information Security Management System.
4. The Company safeguards itself against losses arising from collaboration by monitoring Associates on an ongoing basis as regards their compliance with security requirements. The Proxy for the Information Security Management System stipulates the requirements for monitoring Associates.
5. Any Associate violating the security regulations will be subject to the appropriate sanctions, such as termination of their contract, contractual penalties and/or being reported for a suspected criminal offence, in accordance with the applicable law.

General principles

Materials and measures used when a contract is terminated

1. Any and every permission issued to an Associate must be revoked no later than twenty-four hours after the contract has terminated. The Member of Staff responsible for coordinating the collaboration with that Associate is responsible for cancelling the permissions.
2. As soon as a collaborative relationship is terminated, the Associate must return all the equipment they hold. The Member of Staff responsible for coordinating the collaboration with that Associate is responsible for the return of the equipment, which must be carried out no later than the moment at which the contract comes to an end.
3. The return of data is carried out in accordance with PRO#102 Procedure for conveying/returning data EN Rev.A.

General principles

Security in contracts with suppliers

Contracts with Suppliers of services should be documented and contain the necessary requirements in respect of information security. The basic provisions should:

1. stipulate the information to be conveyed or made available and the method for conveying it or gaining access to it;
2. state the classification of the information (business secret) and, if necessary, reflect the Company's classification scheme and that of the Supplier;
3. include the obligation on the part of the parties to implement the agreed set of safeguards, including access control, reviewing efficiency, monitoring, reporting errors and conducting audits, as necessary;
4. set out the principles for the use of information, including impermissible use, if necessary;
5. include a list of the Supplier's staff authorised to use or receive information or organisational procedures or the terms and conditions for authorisation and its withdrawal as regards access to the Company's information or its receipt by the Supplier's Members of Staff;
6. stipulate the requirements and procedures for managing incidents, particularly as regards notifications and collaboration while proceeding with an incident;
7. specify the training and requirements in respect of knowledge of the correct information security procedures and requirements, such as responding to an incident, authorisation procedures and so forth;
8. stipulate the regulations relating to assigning tasks to be carried out by other Sub-Suppliers;
9. ensure that Suppliers will both promulgate the Company's security requirements along their entire supply chain and insist that they are met;
10. include the Supplier's obligation to meet the Company's security requirements;
11. ensure that procedures are in place for continuing to process information if the Supplier is unable to provide the products or services;
12. ensure that critical components of the services and their origins can be traced along the supply chain.

General principles

Monitoring and reviewing Suppliers' services

The monitoring and reviewing of Suppliers' services is intended to ensure that the terms and conditions for information security, as set out in the relevant contracts, are being complied with and that Suppliers are managing incidents and problems correctly.
At the very least, the contracts should:

1. provide for the monitoring of the efficiency level of the services and facilitate verification of compliance with the contract;
2. include the resolution and management of any and every problem identified;
3. provide for the analysis of aspects of information security in the Supplier's relationship with their Sub-Suppliers;
4. ensure that the Supplier maintains the appropriate efficiency of a service, along with plans and actions designed to ensure that the agreed levels of service continuity are retained following serious breakdowns or emergencies.

General principles

Changes to Suppliers' services

The management of changes in the services provided, including upholding and improving existing security policies, procedures and security measures, should take into consideration both the criticality of the relevant systems and business processes and a risk assessment.

Before being implemented, every change should be analysed from the angle of potential risk. The implementation of a change should be agreed with, and accepted by, the appropriate person as per the assigned authorisations, responsibilities and duties.
A history of changes should be kept.

Responsibility, authorisations and permissions

The Asset Owner is responsible for stipulating the principles for exchanging information with service Suppliers.

The Member of Staff coordinating the collaboration with an Associate is responsible for ensuring the requisite protection of any information exchanged and for supervising the activities of external parties throughout the duration of the Associate's contract.

Abbreviations

n/a

Appendices

Appendices:

FOR#001 General Terms and Conditions for Collaboration

POL#015#FOR#002 Information Classification EN Rev.E

POL#015#FOR#003 Supplier Evaluation Spreadsheet EN Rev.E

POL#015#FOR#004 Internet Service Providers EN Rev.E

POL#015#FOR#005 Hardware Suppliers EN Rev.E

POL#015#FOR#006 Cloud Service Providers EN Rev.E

POL#015#FOR#007 Verification Questionnaire for Processing Entities EN REV.E

Related documents:

Słownik pojęć w Zintegrowanym Systemie Zarządzania - Dictionary of terms constituting part of the Integrated Management System

POL#016 Access Control Policy EN Rev.D

PRO#047 Procedure for Selecting Cloud Service Providers EN Rev.A

PRO#102 Procedure for conveying/returning data EN Rev.A.

PRO#112# Procedure for Selecting Suppliers EN Rev.B

Thank you!

MakoLab