Information Security Policy for Supplier Agreements

Purpose

The objective of this Policy is to protect any information assets or data belonging to Hyris to which third party supplier access (or potential access) is given.
This policy is compliant with the internal regulations of the company, the requirements of the current local, national and international law as well as the requirements of ISO/IEC 27001:2013.

Scope

This Policy sets out the requirements which must be adhered to when engaging any third party which has access to any information asset or information which belongs to Hyris.

This policy applies to any type of contractual or other arrangement with a third party where data or information are exchanged or are given access to.

Before agreements

Hyris, in order to assure the continuity of the security of the information involved, reserve the right to collect information about internal security practices of the third party.

Agreement's requirements

Every agreement within the scope of this policy must be regulated by the stipulation of a contract and this contract (or any other annex to the contract) must address the requirements expressed in this policy in term of security of the information exchanged during the agreement.

All the contractual agreements between Hyris and third parties must be in respect with local, national and international laws and ethics.

The information shared by Hyris, or to which the third party get access to, will remain property of Hyris unless otherwise stated.

The third party must oblige not to disclose any information received during the agreement and must be obliged to conserve it.

If there is the need of sharing an information with an entity outside the agreement the sharing part must get written consensus by the owner of the data that must be shared.

Hyris S.r.l.
Corso Garibaldi, 60
20121, Milano (MI)
Italia

P.IVA: IT11809530964
+39.02.82951302
office @hyris.net
https://www.hyris.net

If access is needed to Hyris facilities and/or Hyris System or Software this access must be agreed and regulated inside the contract.

The assets used to gain access that will be provided by Hyris must be treated by the third party as sensible and conserved as such.

Within the duration of the agreements Hyris must reserve the rights to audit the access rights granted to the third party and, eventually, previously disclosed internal security procedures.

Every incident regarding shared information or asset must be communicated to Hyris using the established means of communication within the limits expressed by local, national and internal laws and never beyond 72h from the incident.