ELA'S EXTERNAL PARTIES SECURITY PROCEDURE

1. Scope

1.1 Epure, Lizac si Asociatii ("ELA") maintains adequate security of its information processing facilities and information assets in relation to external parties. All external parties who need to access any organisational information assets are subject to this procedure.

1.2 ELA has (or may have) external party agreements with the following categories of organisations, all of whom are covered by this procedure; risks may be assessed for external parties as individual organisations or as categories, depending on the level of risk involved:

a. Service providers,
b. Customers,
c. Outsourcing suppliers (facilities, operations, IT systems, data collection, call centers, others),
d. Consultants and auditors,
e. Developers and suppliers of IT systems and services,
f. Cleaning, catering and other outsourced support services,
g. Temporary personnel, placement and other (casual) short-term appointments.

2. Responsibilities

2.1 The Managing Partner is required to ensure that external parties have entered into a formal external party agreement under this procedure, and that transfers (of information, information processing facilities, and any other information assets or personnel) are planned and executed without a reduction in the level of security that existed prior to commencement of the transition.

2.2 The Managing Partner is responsible for ensuring that the security controls, service definitions and delivery levels included in external party agreements are implemented, maintained and operated by the external party.

2.3 The IT Manager is responsible for carrying out risk assessments where required by this procedure.

3. Procedure

3.1 Where there is a commercial need for working with external parties, ELA shall ensure that its information security is not reduced; access to organisational assets is not granted until a risk assessment has been completed, appropriate controls identified and implemented.

4. Risk identification

4.1 ELA shall carry out a risk assessment to identify risks related to external party access and the possible need to complete a data protection impact assessment.

4.2 The risk assessment shall identify and document, for each external party:

a. The information processing facilities and information assets the external party will access.
b. The type of access the third party will have – physical access and/or logical access (identifying the assets that will be accessed), whether the access is taking place on site or off site and the exact location from which access will be made.
c. The value and classification of the information that will be accessed.
d. The information assets that the external party are not intended to access and which may require additional controls to secure.
e. The external party's personnel, including their contractors and partners, who will or might be involved.
f. How external party personnel are to be identified.
g. How the external party will process, communicate and store information.
h. The impact to the external party of access not being available when required, or of inaccurate or misleading information being entered, received or shared.
i. Any legal, regulatory or other contractual issues that should be taken into account with respect to the external party.
j. How the interests of other stakeholders might be affected by any decisions.

5. Controls

5.1 ELA shall agree with the external party those controls that the external party is required to implement and shall document them in an agreement that the third party signs. The obligations on the external party include ensuring that all its personnel are aware of their obligations.

5.2 The agreements between ELA and external parties (whether suppliers or customers) shall include clauses in respect of:

a. The reference to ELA's Information Security Policy.
b. The controls identified as required through the risk assessment process, which may include procedures and technical controls.
c. A clear definition and/or description of the product or service to be provided, and a description of information to be made available.
d. Requirements for user and administrator education, training and awareness.
e. Provisions for personnel transfer.
f. Description of responsibilities regarding software and hardware installation, maintenance and de-commissioning.
g. Clearly defined reporting process, reporting structure, reporting formats, escalation procedures and the requirement for the external party to adequately resource the compliance, monitoring and reporting activities.
h. Physical controls, including secure perimeters.
i. Controls against malware.
j. The reference to ELA's Access Control Policy.
k. Information security incident management.

l. The right to monitor and audit performance (including of the third party's processes for change management, vulnerability identification and information security incident management), to revoke activities, and to use external auditors.
m. Service continuity requirements.
n. Liabilities on both sides, legal responsibilities and how legal responsibilities (including data protection and privacy) are to be met.
o. The protection of intellectual property rights, including copyright.
p. Controls over any allowed sub-contractors.
q. Conditions for termination / re-negotiation of agreements, including contingency plans.

6. Information transfer agreements

6.1 Additional controls must (subject to an individual risk assessment in relation to each proposed agreement) be considered where the contract is for the transfer of information or software:

a. Specific management responsibilities and procedures on each side for notifying transmission, dispatch and receipt and any specific controls associated with each action.
b. Procedures to ensure non-repudiation and to ensure traceability.
c. The required standards for packaging and means of transmission.
d. The agreed labeling system.
e. Courier selection and identification methods.
f. Escrow agreements.
g. How information security incidents (loss of or damage to an information asset in transit) will be managed.
h. Data protection, copyright, software licensing.
i. Any technical standards that are required for recording or reading software or information.
j. Any other special controls, such as cryptography.

7. Managing changes to third-party services

7.1 ELA may need to agree changes to external party contracts and agreements to take account of changes that it makes to, or as a result of:

a. the services it currently offers to its clients;
b. new applications and systems it has developed or acquired;
c. modifications, changes or updates to its own policies and procedures;
d. new or amended controls arising from new risk assessments or information security incidents.

7.2 The external party may need to request changes to the contract in order to implement:

a. Changes or improvements to their networks or other infrastructure.
b. New or improved technologies, new products or new releases of current products.
c. New development tools, methodologies and environments.
d. New physical locations or physical services.

e. New vendors or other suppliers of hardware, software or services.

7.3 Any changes that may be required are subject to a new risk assessment (taking into account the criticality of the business systems involved) and review of the selected contro.

7.4 New controls, or changes to existing controls shall be identified, authorised, agreed with the third party, and made the subject of an agreed variation to the existing contract.

7.5 The Managing Partner shall be responsible for ensuring that the revised controls are implemented and incorporated into the existing review and monitoring arrangements.

Document Owner and Approval

The Managing Partner is the owner of this document and shall ensure that it is kept up to date. A current version of this document is available to all members of staff on ELA's website on page "Data Protection", section "Policies & Procedures". This policy was approved by Decision of Partners on 15.02.2018 and is issued under the signature of the Managing Partner.

Signature: Doru Epure – Managing Partner Date: 15.02.2018