ELA'S INFORMATION SECURITY POLICY

The Partners of **Epure, Lizac si Asociatii SCA** ("ELA"), located at 41 Strada Frumoasa, Sector 1, Bucharest, a law firm organized as a professional association, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image.

ELA's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks. ELA's IT Consultant is responsible for the management and maintenance of a risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are specifically defined and are supported by specific documented policies and procedures.

ELA aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All employees and collaborators of ELA are expected to comply with this Policy and will receive appropriate training. The consequences of breaching the information security policy are set out in ELA's disciplinary policy and in contracts and agreements with third parties.

This Policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this Policy, achievement of adequate information security shall mean ***Preserving of the availability, confidentiality and integrity of the physical and information assets*** belonging to ELA.

The 'preservation' factor implies:

- that management, all full time or part time employees, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security and to report security breaches. All employees and collaborators will receive information security awareness training.

The 'availability' factor implies:

- that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and ELA

must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information.

The 'confidentiality' factor implies:

- that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to ELA's information and its systems (networks and websites).

The 'integrity' factor implies:

- safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency and data backup plans and security incident reporting.

The 'physical assets' include:

- ELA's computer hardware, data cabling, telephone systems, filing systems and physical data files.

The 'information assets' include:

- information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of ELA.

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