ELA'S USER ACCESS MANAGEMENT PROCEDURE

1. Scope

The access rights of all individual users or user groups to any information assets, systems or services of Epure, Lizac si Asociatii SCA ("ELA") are managed in accordance with this procedure.

2. Responsibilities

2.1 The IT Manager is responsible for administration of allocated and authorised individual user or user group access rights in conformity with this policy.

2.2 The HR Manager is responsible for initiation and administration of new and changed user access requests (user agreements) and user training.

2.3 All of ELA's managers are responsible for authorising access requests as being in line with business and organisational security policy and procedure.

2.4 Asset owners are responsible for authorising access requests to their information assets as being in conformity to the security requirements of the asset.

2.5 The IT Manager is responsible for reviewing user access rights in line with the review requirements of the GDPR.

3. User registration and de-registration

3.1 User agreements contain statements of access rights and statements indicating that users have understood and accepted the conditions of access.

3.2 Every user's proposed access rights are documented in a User Agreement, which details the systems/services/applications/information assets to which access is to be granted, together with the level of access that is to granted, taking into account ELA's Access Control Policy.

3.3 The system/asset owner has authority to grant access to the system/asset which he/she owns.

3.4 The User Agreement is then signed by the user and passed to the IT Manager, and the username/user ID is created and administered.

3.5 The IT Department maintains a list of authorised users, administers changes in access rights and removes users.

3.6 The disciplinary policy will be invoked in cases of attempted unauthorised access.

4. Privilege management

4.1 Privileges are allocated to a different username than that allocated for normal use.

4.2 Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated in an e-mail from the user concerned to the IT Manager, which sets out the reasons why the privilege is required and the length of time for which it is required.

4.3 The IT Manager retains a log of all privileges authorised and allocated and checks on a monthly basis that they have been de-activated as specified in the original request.

5. Password management

5.1 The allocation of passwords is formally controlled.

5.2 User password responsibilities are documented in their signed User Agreements.

5.3 Users are initially issued with a unique temporary password which they are forced to change at first logon.

5.4 Monthly password changes are enforced, re-use of passwords is prohibited for 16 subsequent attempts, and seven-character alphanumeric passwords are required.

5.5 Users who need to be issued with a replacement password must first obtain the written authorisation of their process manager (who is required to confirm the identity of the user); this written authorisation must be presented to the IT Department before a new unique temporary password can be issued.

5.6 Passwords are stored stored separately from application system data and are protected.

5.7 The default passwords on all new equipment are changed to conform with ELA's password requirements before the equipment is brought into service.

6. Review of user access rights

6.1 Access rights are reviewed monthly and their adequacy is confirmed; any changes that need to take place are actioned.

6.2 User access rights are reviewed when a user's role or location within ELA changes in any way. If the access rights need to change, a new user agreement is issued, in line with this procedure, setting out those access rights.

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