ASI elementAl System Users Policy

This Policy was adopted on 16 January 2020.

Purpose of the Policy

To control user access to ASI's Assurance Platform, elementAl, developed by ASI on the Knack SaaS system.

Policy and Procedures

All elementAl users (outside of the ASI Secretariat) are assigned to only one user role, which is one of a Member, Auditor, Guest or ASI Secretariat. The ASI Secretariat has access to other user roles for test purposes.

Adding users:

Member users will be added from:

- Member contacts provided in ASI membership application forms.
- Additional member contacts requested or confirmed by a member's ASI primary contact or elementAl contact.
- Additional member contacts requested by a person, including elementAl online requests confirmed by the member's elementAl contact or if not specified, the member's ASI primary contact.
- Following review of a request from an ASI Member (ASI's primary contact) when the Registered Specialist has been commissioned by the Member to assist with its Self Assessment.
- Note that member users must match the member email domain (eg jane@alucompany.com where 'Alucompany' is the ASI member). Private email addresses are not permitted. The only exceptions are:
    - elementAl users in China who experience issues receiving elementAl emails to their company email address.
    - ASI Registered Specialists who assist Members during their certification process. Members are requested if possible, to provide a member email address for the duration of the specialist's engagement. Members are also reminded to inform the ASI Secretariat when the engagement is complete so the specialist's access can be removed.

Auditor users will be added from:

- Auditor contacts provided in ASI auditor accreditation application forms, subject to ASI approval and completion of training requirements.
- Additional auditor contacts – support personnel or Registered Specialists requested or confirmed by an auditor's ASI primary or elementAl contact, subject to ASI approval.
- Note that auditor users must match the audit firm email domain whenever possible (eg john@auditinc.com where 'AuditInc' is the ASI accredited auditor). The exception to this is:
    - When an auditor is a sub-contractor and has not been provided with an email address in the audit firm.
    - When an auditor is associated with multiple audit firms, a separate auditor user will be added for each audit firm, each with a unique email address.

Guest users (a special subset of Member users):

- May be invited by the ASI CEO at her/his discretion, for example potential members and key stakeholders/partners, to enable them to explore the ASI assurance process within their own guest organisation's account.

ASI Secretariat users:

- Will be added by the ASI CEO and must have '@aluminium-stewardship.org' as their main email address.
- If ASI staff require an additional testing account for app building or training purposes, a non-ASI email address is permitted for use in a test organisation setting.

Removing users:

Users' accounts will be promptly made inactive for any of the following reasons:

- As requested by the user.
- As requested by an ASI primary contact or elementAl contact.
- No longer employed by the organisation. ASI will monitor regular communications for notifications of change of employment.
- Completed the assignment that required special elementAl access (such as for a Self Assessment or an Audit).
- In the case of Guest users, as determined by the CEO in the context of the purpose of the Guest access.
- In the case of any deliberate abuse of the system and/or staff.

Where ASI members do not maintain their membership, the associated users' accounts can become Guest Users on request.

Where ASI audit firms do not maintain their ASI Accreditation, the associated users' accounts will be made inactive.

User responsibilities:

Users of elementAl are responsible for the security practices and protection of their devices and logins. All users must:

- Choose strong passwords for their elementAl accounts.
- Advise ASI of any staff or responsibility changes in their organisation that affect elementAl accounts.
- Implement up-to-date antivirus software on their devices.
- Regularly update their operating system, business software and applications (e.g. web browsers) to ensure the latest security patches are in place.

Revision history
Version 1 – adopted 19 September 2017
Version 2 – adopted 16 January 2020