APSCA

ASSOCIATION OF PROFESSIONAL
SOCIAL COMPLIANCE AUDITORS

DATA
SECURITY POLICY

1.0 PURPOSE

APSCA must protect restricted, confidential or sensitive data from misuse and loss to avoid reputational damage and to avoid adversely impacting our Member Firm(s) and/ or Member Auditor(s). The protection of in scope data is a critical business requirement, yet flexibility to access data and work effectively is also critical.

This policy covers the security outline for the APSCA web application data platform provided by Knack, and hosted on Amazon Web Services infrastructure (AWS), and the areas of the security best practice activity:

1. **Confidentiality:**
   ASPCA's data collection, privacy and security standards meet international requirements. APSCA ensures Members' information is maintained in a way which protects the privacy of the Member.
2. **Integrity:**
   To ensure the integrity of Members' data, only the APSCA Data Administrator and Director of Systems Management will have access to make changes to the information held in the APSCA web application data platform *(Knack)*.
3. **Availability:**
   Members will have access to their data with the ability to review and request changes or deletions via a request to the APSCA Data Administrator.

Data contained by *Knack* is the most valuable asset for APSCA and its Members, as a result, this policy outlines the requirements of our web application data platform *(Knack)* and the use and privacy of data held and managed by APSCA.

2.0 SCOPE

- APSCA's web application data platform (Knack) stores Members' data including sensitive data, personally identifiable information (PII) and company data.
- APSCA's Data Security Policy will define the requirements for the handling of this information and user behaviour requirements.

3.0 ABBREVIATION / DEFINITIONS

- **APSCA** – Association of Professional Social Compliance Auditors.
- **Member** – APSCA Member Firms and/or Member Auditors.
- **PII** – Personally Identifiable Information, is any information about an individual auditor that can be used directly, or in connection with other data, to identify, locate or contact that individual auditor. Such information includes educational and/or employment history.
- **AWS** – Amazon Web Services (platform on which APSCA data is hosted).

4.0 REFERENCES / RELATED DOCUMENTS

- T-006 APSCA Data Dictionary
- D-016 APSCA Data Management Process

5.0 DATA ADMINISTRATOR

APSCA has an appointed Data Administrator. This Administrator is responsible to follow the principles and procedures contained within this policy including the handling of restricted, confidential or sensitive Member data.

6.0 DATA ACCESSIBILITY AND DISCLOSURE

APSCA membership data is accessible only by the relevant APSCA team. This team is held accountable to this policy and are bound by a signed Confidentiality Agreement.

7.0 DATA PROTECTION OFFICER

APSCA has an appointed Data Protection Officer. The Data Protection Officer is responsible to oversee APSCA's systems and processes to ensure the handling of data is in accordance with this policy and will also act as a point of contact for any queries, concerns or reporting of misconduct by APSCA employees handling this data.

8.0 POLICY

8.1 APSCA's web application data platform *(Knack)* utilises Amazon based cloud servers which stores data in an encrypted state. The data will remain the property of APSCA and will not be used for any other purposes other than to manage APSCA membership whilst conducting normal business. Access to Knacks's security statement and policies are to be found here - https://www.knack.com/tour/security

8.2 Amazon Web Services (AWS) which hosts *Knack's* cloud based servers, has stringent data security policies and undertakings – their credentials, certificates and statement are found under the Assurance Programs Section here - https://aws.amazon.com/compliance/

8.3 APSCA's web application data platform (*Knack)* is to perform vulnerability scans, security testing and auditing services as part of APSCA's subscription contract.

8.4 Should APSCA be advised that a data breach has been detected, APSCA is required to notify all affected Members, APSCA Executive and Stakeholder Boards and the APSCA Data Protection Officer within 72 hours.

8.5 Members can request a copy of their company data or PII in the form of an Excel report to enable the Member to transfer the information to another source of their choice. This will be performed by the APSCA Data Administrator within 21 days.

8.6 Members can request, for review, a copy of their company data or PII in the form of an Excel report by contacting the APSCA Data Administrator. This report will be provided within 21 days.

8.7 Members can request that any inaccurate company data or PII be corrected and/or erased from APSCA's web application data platform *(Knack)*. This will be performed by the APSCA Data Administrator within 21 days.

8.8 APSCA will retain records of all Members' company or PII, for a period of 7 years from termination of the Member's APSCA membership.

8.9 Members can refuse permission for APSCA to use or process their company data or PII.

8.10 Member's company data or PII cannot be shared with other parties unless consent, from the relevant member, is received by APSCA to share that information. This company data or PII would be in the form of an Excel report and performed by the APSCA Data Administrator.

8.11 If APSCA is required by law or receives any order, demand, warrant or any other document requesting or purporting to compel the production of Member company data or PII, APSCA shall not produce this information for at least 48 hours. The relevant Member will also be notified of this demand prior to the information being provided. This company data or PII would be in the form of an Excel report and performed by the APSCA Data Administrator.

8.12 In scope data and data classification level for Member Firms and Member Auditors is defined as follows:

APSCA MEMBER FIRM

Data Classification	Content	Visibility
Light / Open	▪ APSCA Membership Number (APSCA defined) ▪ Membership Status (APSCA defined) ▪ Company Name ▪ Company Business License Number ▪ Company Address, Phone, Fax, Website address ▪ Year of Foundation of Business ▪ Countries where Member Firm conducts Social Compliance Audits.	Public
Moderate / Restricted	▪ Member Firm Contact Name ▪ Member Firm Contact Mobile ▪ Member Firm Contact Email ▪ Member Firm Social Compliance Revenue Band ▪ Member Firm Category of Membership ▪ Member Firm Ownership Details ▪ Member Firm Scope of Business ▪ Member Firm National Prohibition, Litigation and\or Arbitration Details ▪ Member Firm Internal Policies relating to: Impartiality, Integrity, Conflicts of Interest, Confidentiality, Anti-Bribery, Fair Marketing ▪ Industry Accreditation Details (including scheme accreditations, brand audit programs) ▪ Details of Special Services eg. Training ▪ Scanned Signed Code of Professional Conduct ▪ Scanned Signed Confidentiality Framework Agreement ▪ Consent for APSCA to store and maintain Member data	Member Firm (Minimum data set for participation as APSCA Member Firm)

Data Classification	Content	Visibility
Enhanced / Secure	▪ Industry Comment / Feedback ▪ Disciplinary Issues (including any allegations / investigations)	APSCA Team

APSCA MEMBER AUDITOR

Data Classification	Content	Visibility	Business Justification
Light / Open	▪ Member Auditor Name	Public	Method to identify Auditor Name in English
	▪ APSCA Membership Number (APSCA defined)		N/A
	▪ APSCA Auditor Level (APSCA defined)		
	▪ APSCA Membership Status (APSCA defined)		
	▪ Auditor Image		Method to identify Auditor
Moderate / Restricted	▪ Name in local language, if applicable ▪ Other names known by, if applicable	Member Auditor (Minimum data set for participation as APSCA Member Auditor)	Method to identify Auditor
	▪ Gender		Triangulate information to avoid duplication
	▪ Auditor home address		
	▪ Auditor personal email address		
	▪ Work email address		Ability to contact/ communicate with Auditor
	▪ Mobile		Triangulate information to avoid duplication
	▪ Member Firm Name(s), if applicable		Link auditor to each firm they are working with– this may be multiple firms, to alert should status change
	▪ Employment status (Employed, Subcontractor, Freelance)		May impact on invoicing for membership, impacts on audit firm "status" as based on registered Auditors
	▪ Languages Spoken/Written, including proficiency level		Required

Data Classification	Content	Visibility	Business Justification
Moderate / Restricted	▪ Education / Qualifications	Member Auditor (Minimum data set for participation as APSCA Member Auditor)	As per Competency Framework step required in eligibility to sit for APSCA CSCA exam & maintain APSCA CSCA status
	▪ Social Compliance Experience Details		As per Competency Framework step required in eligibility to sit for APSCA CSCA exam & maintain APSCA CSCA status Optional
	▪ Industry Experience Details (including scheme accreditations, brand audit programs)		
	▪ Training, including CPD		
	▪ Special Skills		
	▪ Scanned Signed Code of Professional Conduct		As per Competency Framework step required in eligibility to sit for APSCA CSCA exam
	▪ Consent for APSCA to store and maintain Member data		
Enhanced / Secure	▪ Detailed Auditor File (including any allegations/ investigations)	APSCA Team	
	▪ Industry Comment / Feedback		
	▪ Disciplinary Issues		
	▪ Date Relationship with Firm Concluded \ Reason		

REVISION HISTORY

Date	Revision #	Page (s)	Description of Change(s)	Author	Authorizer	Superseded Document
20 Sep 2017	2	4 - 5	Included APSCA Member Firm Data Classification Table	Julie Shaw	Rona Starr	V1 – 11 Aug 2017
20 Sep 2017	2	4 - 6	Updated APSCA Member Auditor Data Classification Table	Julie Shaw	Rona Starr	V1 – 11 Aug 2017
15 Dec 2017	3	2	2. Integrity - updated	Julie Shaw	Rona Starr	V2 – 20 Sept 2017
15 Dec 2017	3	3	6.0 Data Accessibility & Disclosure - updated	Julie Shaw	Rona Starr	V2 – 20 Sept 2017
15 Dec 2017	3	4-5	APSCA Member Firm Table – update to Light Open / Moderate/Restricted & Enhanced Secure Section	Julie Shaw	Rona Starr	V2 – 20 Sept 2017
15 Dec 2017	3	5-6	APSCA Member Auditor Table – update to Light Open / Moderate/Restricted & Enhanced Secure Sections	Julie Shaw	Rona Starr	V2 – 20 Sept 2017
1 Feb 2018	4	5	APSCA Member Auditor Table – Update to Light Open Section	Julie Shaw	Rona Starr	V3 – 15 Dec 2017

APSCA

ASSOCIATION OF PROFESSIONAL
SOCIAL COMPLIANCE AUDITORS