Knack (elementAl) Security Information

Last updated: 16 January 2020.

Purpose of Documenting Security Information

To summarise relevant security information of the Knack platform, on which ASI's Assurance Platform 'elementAl' has been developed, and make it available to all users.

Information on Knack's security is available at: https://www.knack.com/tour/security

Server locations

ASI's applications and data are hosted on Knack's EU-based data cluster in Frankfurt, Germany.

Infrastructure

Knack uses Amazon Web Services (AWS) to power its platform. Amazon Web Services is considered the industry leader in cloud services and is trusted by organisations like DOW Jones, Pfizer, and the CDC.

- Compliance: AWS environments are continuously audited, with certifications from accreditation bodies across geographies and verticals, including SOC 3 and ISO 27001 Certifications.
- DDoS Mitigation: AWS provides a robust platform that is pre-built to mitigate some attacks and allows Knack to react quickly to spread out impact if there is an attack.
- Redundancy features: Knack uses AWS features like Auto-Scaling and Elastic Load Balancing to ensure that systems remain online.

Platform-level security features

Key aspects include:

- Encryption: All data is encrypted while in transit and when stored on Knack's servers. Bank-level encryption technology is used, both SHA-256 and AES-256.
- Back-ups:
    - Database records are backed up by Knack on a daily basis at 8am GMT and are retained for 7 days before being overwritten. This means that this Wednesday's backup will overwrite last Wednesday's. Restoring the previous Wednesday's data is not possible after it is overwritten.
    - App structures are backed up by Knack every 12 hours at 7am and 7pm GMT and are retained for 7 days before they're overwritten. Knack also does a weekly backup of the app structure every Friday and keep that for a year.
    - Edit history logs viewable in the Knack Builder are retained for 3 months.
- Redundancy: Knack mitigates database failures by storing data in multiple databases, so if one database goes down the other databases can pick up the slack. Physical backup files are stored in a separate location from the servers as a final safeguard in case of major catastrophe.
- Firewalls: Knack uses firewalls to protect every virtual server, database, and load balancer to ensure that only authorised traffic is accessing those resources.
- Development Silos: Knack engineers work in a development environment that is completely separated from any live data.

App-level security features used by ASI

ASI has implemented the following app features in the design and development of elementAI:

- **Password Protection:** Only authenticated users can access elementAI.
- **Password Encryption**: All user passwords are double encrypted and hashed with a salt, which prevents dictionary attacks and adds an extra layer of security.
- **Roles & Permissions:** Roles and permissions are defined for each user, restricting access at the individual page level.
- **Record Level Security:** Each logged-in user can only access the records that are connected to them.
- **Version Tracking:** Edit history logs, for the elementAI dashboards, the Knack builder, and the API, are retained for 3 months and viewable in the Knack builder.
- **Secure Files**: Files are stored behind logins so only authenticated users can view and download those files.

Knack Policies

Knack have implemented security policies around data privacy and under what circumstances the Knack team can access data.

- **Privacy**: Knack maintain a Privacy Policy that outlines their commitment to respecting privacy and the privacy of the information in ASI's account.
- **Data ownership:** Knack has no ownership of users' data.
- **Access to data**: Knack employees do not have access to the data stored in ASI's account, unless the relevant user agrees to make it accessible. If the Knack team needs to access your data for support services, they only do this at your and ASI's request and when it is necessary to resolve the issue.
- **NDA and Confidentiality:** Each Knack employee signs non-disclosure and confidentiality agreements that provide legal backing for the obligation to keep your data private and confidential.
- **Training**: Each Knack employee undergoes training and instruction on data access and privacy and how to securely handle customer requests for account or billing access.
- **Access Logging**: Every access request to your data by a Knack employee is logged and time-stamped. Knack can confirm exact access by the Knack team to any data in the unlikely case that this log is needed.
- **VPN Access:** All access by Knack employees to customer data is governed by a secure virtual private network. This access is monitored and can be revoked at any time.

Personal information

ASI's Privacy Policy explains how ASI collects your personal information, what we do with it and how we protect it. The Policy is available within elementAI and on the ASI website.

ASI's elementAI platform needs to store your name and email address to enable account authentication and login access. You may also wish to provide additional information about yourself such as your role title, languages spoken and gender under your 'User Details'.

Commercial information

The elementAI platform is designed to support the assurance process for ASI certification. Users are able to upload notes, files and images as supporting material for assessments of conformance against ASI Standards. This can then efficiently be made available to a chosen ASI Accredited Auditor.

Users should make their own decisions as to the sensitivity of any information they wish to upload into elementAI. If users have concerns about uploading information, an alternative is to make relevant information available to auditors when they are on site or via other communication channels.

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