noggin requestor

Noggin Requestor Technical FAQ's

Technical platform

Noggin's platform uses an innovative architecture, designed using our real-world experience in building software in the emergency and crisis management industry. It provides a single-page web application for both desktops and hand-held devices, that connects to our servers using web-sockets. This design means that the application is tolerant of intermittent connectivity, and new information can be pushed from the server when it's available - rather than when you next refresh.

Resilience and scalability

Noggin's servers are located in three availability zones within Amazon Web Services. The servers are arranged in a horizontally scalable, high-availability cluster. Should a wide-scale emergency hit, we can scale horizontally to meet demand. Should a zone have an outage, the others will automatically shoulder the load. This ensures that no matter how many users, or what the crisis is, we can handle the load.

Security

Noggin's platform is hosted in Amazon Web Services' (AWS) data centres. These provide numerous security & privacy certifications, and legal and regulatory compliances. These include FedRAMP, FIPS, DoD SRG, Cyber Essentials Plus, IRAP, ISO 9001, 270001, 27017 & 27019, and SOC 1, 2 and 3. They also comply with data protection and privacy laws & regulations in the USA, Canada, Australia, UK, EU and New Zealand. The current set of compliances and certifications is located at *https://aws.amazon.com/compliance/*.

All data to and from the Noggin platform is securely encrypted using TLS v1.2. All users are verified through their email address, which must be unique. Their email address is also used as a basis for password recovery. Each user is placed in an access group which then determines what they can and can't do.

Noggin uses a password strength estimator, that through pattern matching and conservative estimation, recognises and weighs 30,000 common passwords, common names and surnames. It references US census data, popular English words from Wikipedia and US television and movies, and other common patterns like dates, repeats, sequences, keyboard patterns, and l33t speak.

Data integrity

Noggin's platform keeps an audit trail of every change that is made, and retains every version of every record. Each new version contains a reference to its predecessor, and as a data integrity protection measure, each version is immutable – its primary key is a 256-bit encrypted hash of the record contents. This includes the reference to its predecessor, thereby making the record and its history tamper-proof. Each version is also stored with the date/time of when it was written and the user session that wrote it, so every change can be traced to a specific user.

Minimum requirements

Noggin's platform is designed to work on the following desktop web-browsers:

- Chrome XX+
- Firefox XX+
- Safari XX+
- Edge XX+
- Internet Explorer 11

And the following mobile web-browsers:

- Chrome XX+
- Safari iOS XX+

No plugins are required (e.g. Java or Flash).

noggin