Hosting and Security

- Hosted in Amazon Web Services (AWS) in multiple regions utilising best practise scalability and redundancy configurations
  - AWS London (eu-west-2)
  - AWS Sydney (ap-southeast-2)
  - AWS US East (us-east-1)
- Survey Dynamix can be hosted in any AWS region as required by the customer
  - Encryption at rest available in most instances
- AWS is a world leader in cloud computing security and is compliant with all customer security needs. For more information about the security that AWS provides visit https://aws.amazon.com/security/
- All internet traffic including survey traffic and traffic from 3rd party applications is sent over authenticated and encrypted SSL/TLS connections to ensure that data can only be read by the intended recipients
- Our services utilise the Twilio network for the provision of telephony/IVR services. All communication between our web servers and the Twilio services are via secure HTTP and encrypted via TLS. Other third party providers include:
  - Google Speech Services for Speech to text transcriptions of customer voice recordings
    - Speech to text transaction is optional capability
    - All customer feedback recordings stored in AWS S3 buckets (deleted from Twilio after collection)
- Our full privacy policy can be found at https://surveydynamix.com/privacy_policy
- Our SAAS Terms of Use can be read at: https://surveydynamix.com/terms_of_use

Security FAQ Part 1

- **Access Control: How is access to Survey Dynamix controlled?**
  - Access to Survey Dynamix is through an email address and password combination
  - Programmatic access available through:
    - Oauth
    - Personal Access Tokens
    - Basic Auth (Customer UUID / Auth Token combination)
- **Data accessibility: who can access what and how, what is the granularity of the data restriction if any etc**

  As a Survey Dynamix user we have 3 user roles:

  Agent: The agent role is able to access the dashboard and interaction details reports. Both of these provide full access to survey details including survey meta data and personal information such as phone number (if allowed) and email address of the respondent. Administrators of Survey Dynamix can restrict surveys visible to each agent based on the agent_id associated with the survey interaction. For example if "I am agent123 I can be restricted to see only survey interactions where the agent_id attribute is agent123". An agent can also be granted the ability to see other interactions based on agent id such as team mates. For example agent123 might be allowed to see interactions associated with agent100, agent101, agent103 etc.

  Supervisor: The supervisor role is able to access all survey interaction data from dashboard or the interaction details report. There is no way to restrict a user of this role to a limited set of data.

  Admin: The admin role is able to access all survey interaction data from the dashboard or the interaction details report.

  In terms of Contact Dynamix Pty Ltd staff and their access to the data:

  Where a staff member has a requirement for access to our databases this access is provided through their AWS accounts. Database access is restricted to components of our solution such as our Application Servers and other databases and to registered IAM users. Database access is further controlled by IP address whitelisting and only our office IP address is configured for access.

  Contact Dynamix staff are fully versed in our privacy policy and their related obligations around data access. Some of our staff will access our customer's accounts, as required, to provide support, training or configuraiton. If any private or personal information is seen during these times our staff are aware it must never be relayed to any other person (staff or otherwise) and treated in the utmost confidence.
- **Data storage: where are the data stored, for how long and can it managed**

  All Survey Dynamix customer data is stored in a MySQL database hosted in our AWS account. We have several instances in different AWS regions. Each instance houses the data for customers in that region. Our database environment consists of a database cluster comprising a database WRITER and one or more auto-scaling database READER instances. Database snapshots are taken regularly and stored for backup and restore purposes – this is all managed through native AWS capability.

  Customer data is retained for the life of the customer account. A customer has up to 30 days from the end of the contract to export their data before it is removed from our databases.

  We currently utilise AWS US-East (North Virginia) and EU (London) regions. Encryption at rest database instances are available if required.

  Data can be managed through the API with valid credentials and via the web application UI. It is possible to search for and delete survey interaction data (with cascading deletes) via the API and UI to enable quick compliance with GDPR personal data removal requests (for example).

Security FAQ Part 2

- **Data transmission: where are the data transiting to/from services outside of the AWS instance region?**

  Survey Dynamix -> Web App User
  HTTPS, Authenticated by user account
  Type of data: everything available to the user from the web app

  Survey Dynamix -> Web or Email Survey Respondent
  HTTPS, Unauthenticated
  Type of data: questions, greetings and question responses only

  Survey Dynamix -> Twilio and vice versa
  HTTPS, Authenticated API Access on each request
  Type of data: Questions, greetings and question responses, customer voice recordings, customer phone number, Voice recordings are deleted from Twilio and stored in AWS S3

  Survey Dynamix -> Google Speech Services
  HTTPS, Authenticated API Access on each request
  Type of data: Customer voice recordings, Transcription of voice recording returned to Survey Dynamix
  Note: Voice recording transcription is optional

- **What "Personal Information" is stored in Survey Dynamix?**

  The following is a breakdown of the types of "personal information" Survey Dynamix may store:

  For Survey Dynamix users (we are the Data Controller):

  - First / Last Name
  - Phone number (optional)
  - Email address (mandatory)
  - Timezone

  For Survey Respondents (we are the Data Processor):

  - MANDATORY: Email address or Phone Number (or both if our customer decides to store both). One will be required depending on the survey medium.
  - OPTIONAL: Any other data our customer (Data Controller) decides to associate with survey interactions. This could be literally anything but is at the discretion of our customer. This could be for example CustomerName, Customer CRM ID, Customer Address etc.