

G Cloud 15 Service Definition Document – Open Banking

What is Open Banking?

Open Banking is a facility to allow Councils and other governmental organisations the opportunity to utilise the “Pay by Bank” service. We send a message or QR code that allows the customer to open their banking app (whichever bank they use) and the transfer is already set up for them (including the correct reference on the payment to prevent “orphan payments”).

Back Up and Disaster Recovery

Please see appendix A BCP General principles.

The system runs across 2 data centres in the Midlands, it uses DNS address to offer a seamless failover if we lose a site (Live/Dark configuration). In the event that we lose both sites our RTO is 8 hours, with an RPO of -24 hours.

Onboarding and Offboarding

As part of the implementation process we offer unlimited online training with online trainers available when you start using the service to ensure your first dialling exercise goes out correctly. We build your initial conversational parameters and provide consultation on what other Councils have found to work in particular scenarios.

In terms of off boarding everything is downloaded from the platform and the customer can have all the data from the service prior to us placing it beyond use. We will keep a copy of the data until the system cleanses the account on the weekend after the data becomes one year old.

Maintenance windows

The messages are fully customisable and the service is available during broadcast times (8am-9pm 7 days a week) however once every 3-4 weeks we have a maintenance window on Sunday morning 1.00am to 3.00am.

Service Levels

The customer Helpline is open for telephone enquiries from 9am-5pm Mon-Fri with email support provided out of hours.

After Sales Support

Unlimited training to the first and any subsequent teams utilising the platform ensures a continual transfer of knowledge to an increasing team of Council employees is the usual process followed by Councils once they have adopted the Contact Portal product.

Technical Requirements

Any PC with an internet connection and Microsoft Excel

Outage & Maintenance Management

TelSolutions Ltd have a maintenance window on Sunday morning at 1am to 3am, typically these occur once a month and they don't affect the service as very few people are talking to the Council at this time. During the last 12 months there have been no recorded serious outages but in the event that there are our RTO is 8 hours with an RPO of -24hours.

UK Hosting as standard

Hotcomm host their online dialler in the UK with a failover in the Republic of Ireland.

Access to Data

Although very few Councils choose to leave TelSolutions Ltd, we have a fully developed leaving procedure. All the data we hold is available to our customers at all times through our reporting module. All your data can therefore be accessed at any time, once you have taken all the data that you require we disable the account preventing anyone from accessing the data. We will keep a copy of the data until the system cleanses the account on the weekend after the data becomes one year old.

Security

TelSolutions hold all data extremely securely. The only copy of customer data is held under AES 256bit encryption on the DB server of each individual VLAN our architecture requires a secure transition across 3 F/W secured VPNs each device has IDS, Anti malware and anti-virus and all the logs feed into SIEM that is monitored by both humans and AI in a 24*365 NOC. The data Centres themselves are accredited to ISO 27001 with all the secure physical access these facilities provide.

Appendix A

Business Continuity and Service Outage General Principles:

The following is a statement of the general principles that underpin the Telsolutions Ltd planned resolution to several the likely threats to continuity of our services.

1. DDoS attack.

We have several countermeasures against DDoS courtesy of sitting within the same environment as servers belonging to the MoD, Boeing and a number of defense contractors. These include Cloudflare (for large scale attacks) and 2 Banning platforms, multiple attempts ban the IP address (one looks for potential intrusions, the other bans usage that doesn't appear to be human) and it is unlikely we would be targeted by an organization with the kind of resources (a large Botnet, a foreign govt operator etc.) who could overwhelm these defenses without alerting Cloudflare. However, they potentially could target some of the other tenants and so it is important to note that our provider has committed to bring up their dark site for customers who are unaffected by the DDoS attack in the event another tenant was targeted.

Is it foolproof – no – is it likely we will be targeted – no – are we unusually well protected for an organization of our size – yes?

2. Outage of one or more services.

SMS Messaging

We are totally vendor agnostic on SMS we can switch out a non-performing SMS provider.

Email Messaging

While we can offer a totally vendor agnostic service on email, but in the event of ever heightened security concerns (as the increase in scam and phishing emails continues) most of our customers are asking for unique sub-domains this means we are limited to single email suppliers.

Voice Messaging

Voice Messaging can only be replicated across 2 suppliers using scripts being set up in text to speech, we are in the process of setting this up.

LiveChat/Dialler

These are totally bespoke solutions although the providers we use are selected for their exemplary record of uptime, but if either of them fails there is no possible failover to another platform.

3. Outage of our internal systems.

Our platforms are robust with the main ones (Mail, SFTP & File Server) having significant redundancy and failover across Data Centers. While we can deal with a loss of email, platform loss & loss of SFTP would be more difficult, both are replicated in a live dark site so unless a problem takes down both Maidenhead and Coventry, we should be OK. It is usual to make a further back up and have it sited somewhere totally separate however the lack of a Brexit data agreement is making this impossible with the majority of our UK customer's preferring that they keep all data within the UK until the situation is clearer.

4. Outage of our site in Harlow.

COVID-19 has provided an opportunity to test this capability, the company was able to function without access to the site and only requires phone number porting which can be done remotely (the dialler is hosted in 2 sites neither of which is in Harlow).

5. Loss of key personnel.

Telsolutions has lost 2 senior technical project leaders in the last 5 years as such we have implemented a documentation process that allows all future IT resources to follow our development processes. This has just been tested for the 2nd time with no reported problems.