SCHEDULE J: TOTSCO SECURITY POLICY

VERSION 1 – EFFECTIVE FROM PRODUCTION DELIVERY DATE

Introduction

This **TOTSCo Security Policy** is a schedule to **our agreement** with **you**.

It sets out the security policies **we** apply to ensure the protection of our **hub** and **Services** and all data contained within the **hub** and **Services.**

Messaging Security

1) Within the design of the **production hub** there are several access control mechanisms:

   a) transaction security protection in the form of OAuth2 or API key. These security protocols are the authentication mechanism which ensures that each transaction submitted to the **production hub** is coming from a recognised and authorised CP, and that the returning transaction to **you** is authorised as coming from the TOTSCo **production hub**; and

   b) encryption of the communication sessions (TLS/mTLS) for all transactions.

2) The **production hub** is protected by a Transport Layer Security (TLS) certificate, so that **you** can be sure when you connect, **you** are connecting to the genuine TOTSCo **production hub**, and that also the communication session is encrypted.

3) For added protection **you** can choose to supply to us your own TLS certificate which we will import into the **production hub**, this then ensures that any communication sessions between your platform and the **production hub** are guaranteed to identify the exact authorised endpoint and the sessions will be encrypted using the Mutual Transport Layer Security (mTLS) capability.

4) All hub data is encrypted at rest within the hub database, so during the lifetime of the data within the **production hub** it is always in an encrypted state.

5) **Switching messages** to the **production hub** consist of two parts, an envelope which contains the metadata of the sender, recipient, type of message, it is essentially the routing information for the **switching message**; no sensitive data is contained within the envelope. The second part of the **switching message** is the "payload". Any end-customer details, name, address, phone number and other related personal information are contained in the payload.

6) As soon as a **switching message** is successfully processed the payload part of the **switching message** is deleted. This ensures sensitive data is not being stored within the database for any longer than is required to successfully provide the **production hub Services**. The envelope piece of the **switching messages** is stored within the **production hub** database as **switching metadata**. This is done so that reporting is available, the **switching metadata** is used to help you understand the level of switching being performed through the hub, and to report to OFCOM the level of switches across all UK CPs, all in accordance with **Schedule E – Analytics, Reporting, Archive and Metadata Access Control.**

TOTSCo production hub Security

To safeguard **our production hub** from attacks or malicious acts there are a number of elements in place to protect **our** infrastructure.

1) Intelligent firewalls protect all inbound and outbound network transactions from every **CP** to the **production hub** and vice versa. **You** are required to register any network and endpoint addresses so these can be added to the **production hub** security model and become part of the zero-trust framework.

2) Web Application Firewalls are deployed in front of the **production hub**, and the account-management portal. The WAF monitors for malicious code access attempts, and malicious user activity. Its functionality allows **us** to lock down all application requests to valid legitimate command strings that the **production hub** provides functions for. Through this same functionality any invalid command strings that the **production hub** was not designed to support can be rejected. All command strings are monitored, logged, and reported, attempts to access unauthorised functions.

3) Anti-Virus and Anti-Malware protection is deployed to all infrastructure within the **production hub**. This solution is updated daily to ensure that any malicious code or traffic is inspected, and anything detected is blocked from access to the **production hub**.

4) Host Intrusion Prevention is used on each piece of the hub infrastructure. This ensures that each server is individually firewalled from the others. Specific application ports are opened to ensure the hub functions effectively, but all other ports and traffic is blocked, ensuring that malicious traffic has no ability to traverse the **production hub** infrastructure.

5) A Configuration Management platform is deployed within the infrastructure. This system dynamically monitors the configuration of every server and service within the **production hub**, ensuring that they are all configured to the specified security standards and highlighting any changes to the infrastructure which may reduce the level of security and introduce risk to the **production hub**.

6) A Privileged Access Management platform is deployed within the TOTSCo **production hub** infrastructure. This platform controls all access to privileged admin accounts and the respective systems, giving full audit trails of any access to infrastructure, with relevant authorisation processes behind this. The system also screen records all sessions which can be reviewed and audited at any time by TOTSCo team members. This helps protect against any malicious access to the hub infrastructure and monitors any internal TOTSCo team access as well to protect against any potential insider risk.

7) Vulnerability and Network Testing is being performed on an ongoing basis on the **production hub.** This ensures that vulnerabilities within code, services and servers are detected as soon as possible and can be remediated. This scanning service also ensures that any configuration updates made to the infrastructure has not opened up any gaps in the security standard and increased the **production hub** risk profile.

8) SOC Monitoring and Remediation – A 24x7 security monitoring service will be in place from **OTS go-live date**, reviewing all logs and alerts from **production hub** infrastructure and all the security platforms. With all information being collected into one centralised location, correlation rules are applied to the alerts to help determine any security risks to the **production hub**. Reports are produced daily on attacks seen to the **production hub** infrastructure, these reports are used to help proactively improve the security of the **production hub** and reduce risk on an ongoing basis.

CRM security

We have a customer relationship management system (CRM) which **we** use for all customer service functions and CP reporting. To protect **your** data within the CRM platform there are several controls in place:

1) The CRM platform has its own CRM.totsco.co.uk SSL certificate in place, much like with an online banking session. This means **you** can be sure **you** are accessing the genuine TOTSCo CRM platform and that your web session is encrypted over HTTPS.

2) **Our** CRM database is encrypted, ensuring any data input is always protected.

3) **You** will be asked to register a username and password when being onboarded, each CP user must have their own account within the platform. These must not be shared with other users.

4) **Your** data is segmented and attributed to your login credentials. Only users from **your** organisation (CP) can access that dataset. No other CP can access your records.

5) All access to the CRM by TOTSCo staff members is monitored and recorded using an audit trail. All TOTSCo staff are subject to ad-hoc auditing procedures to review their activity within the CRM.

Hub Reporting

All reporting of **switching metadata** is performed through the CRM platform. Given the level of sensitivity around the collective statistics of the messaging information the CRM security controls are set out below:

1) The CRM system does not have any access to the **production hub** database which contains the **switching metadata** of messaging transaction envelopes.

2) **Switching metadata** pertaining to the envelopes of transactions is stored within the CRM platform so that reporting can be performed at the different levels required.

3) CP specific **switching metadata** is segmented so that an individual CP (**you**) can only see your own transactions within the reporting platform.

4) TOTSCo Business Operations and Customer Service team members are strictly controlled as to their available reports. Access is permitted only for the team to perform their day-to-day duties and nothing further.

5) The TOTSCo Executive team reporting is limited to specific stats regarding the operational levels of the hub and the summarisation of stats for throughput, charging models and other aspects that are required to carry out their day-to-day responsibilities.

6) A Privileged account is used for producing industry wide statistics. This account is only accessible via the PAM security platform, with a full audit trail and session recording.

7) The storing or sending out of any **switching metadata** is strictly controlled through the CRM platform and its access control model.

8) Output Report files are monitored, and their transmission controlled.

a. Required generated files are stored within an encrypted document store that provides tracking of any access to the data.

b. Files that are required to be uploaded to the regulator's secure portal are done so through the privileged access account which is monitored and includes a full audit trail.

c. Any report files generated which are not required after uploading to the regulator and erased from the encrypted document store so as not to create unnecessary risk.