SPECIFICATIONS EXHIBIT

This Specifications Exhibit should be read in conjunction with the Terms and Conditions available at: https://www.tessian.com/wp-content/uploads/2020/07/Terms-and-Conditions.pdf.

SPECIFICATION

Tessian offers four Modules: (i) the Tessian Platform, (ii) Tessian Guardian, (iii) Tessian Enforcer and (iv) Tessian Defender.

The successful operation of the processes described below is subject to a successful connection being established between the Tessian Server and the Local Software.

For the purposes of this Specifications Exhibit:

"**Sender**" means an Authorised User who gives an instruction to Customer's email system to send an email (e.g. by pressing the 'Send' button); and

"**Default Threshold Period**" means 3 seconds for the Add-in and 15 seconds for the Gateway.

Tessian Constructor

Tessian Constructor allows Administrators to implement customisable rules which will specify: (i) criteria to identify certain categories of emails; and (ii) the action which will be taken in respect of any email which meets the specified criteria (e.g. "blocking and auditing any email that is being sent to an external domain containing an .XLSX attachment") ("**Customised Rule**").

If a Sender issues an instruction to Customer's email system to send an email, the following process applies when the Tessian Platform is in use: 1. The Tessian Server is called by the Add-in or Gateway. 2. The Tessian Server determines whether the email meets the criteria specified in the Customised Rule. 3. If the email meets the criteria in the Customised Rule, the Tessian Server will relay a message back to the Add-in or Gateway, which will then perform the specific action of the Customised Rule (e.g. generate an audit log, display a warning notification, block the email from being sent, etc.).

If the Add-in or Gateway cannot connect to the Tessian Server or do not receive a response from the Tessian Server within the Default Threshold Period, the outgoing email will be sent to the recipient without any warning notification being presented to the Sender or any audit log being created.

Tessian Guardian

If a Sender issues an instruction to Customer's email system to send an email, the following process applies when Tessian Guardian is in use: 1. The Tessian Server is called by the Add-in or Gateway. 2. The Tessian Server seeks to detect anomalies which may infer that the email may be sent to an incorrect recipient (e.g. where an email has been inadvertently addressed to the wrong person); 3. If anomalies detected by the Tessian Server imply that the email is being sent to an incorrect recipient, the Tessian Server will generate a warning notification or email which will be presented to the Sender. The warning message will highlight the anomalies detected and give the Sender the option of sending the email or stopping the email from being sent.

If the Add-in or Gateway cannot connect to the Tessian Server or do not receive a response from the Tessian Server within the Default Threshold Period, the outgoing email will be sent to the recipient without any warning notification being presented to the Sender or any audit log being created.

Tessian Guardian uses machine learning to detect anomalies in emails being sent. The email attributes which Tessian Guardian identifies as anomalies are constantly evolving based on learning from previous emails which have been sent or stopped from being sent. As a result, not all warning notifications generated by Tessian Guardian will accurately indicate an incorrect recipient and the Tessian Server will not generate a warning notification or an audit log for all emails sent to an incorrect recipient or an unauthorised recipient.

Tessian Enforcer

If a Sender issues an instruction to Customer's email system to send an email, the following process applies when Tessian Enforcer is in use: 1. The Tessian Server is called by the Add-in or Gateway. 2. The Tessian Server seeks to detect anomalies which may infer that the email may be sent to an unauthorised recipient. 3. If the anomalies detected by the Tessian Server imply that an email is being sent to an unauthorised recipient and the email meets the criteria in the Customised Rule, the Tessian Server will permit one of the following actions to take place:

a) The email will be sent to the recipient and the Tessian Server will generate an audit log which may be viewed by an Administrator but no warning notification will be presented to the Sender.

b) The Tessian Server will send a warning notification to the Sender and give the Sender the option to proceed with sending the email or to stop the email from being sent.

c) The Tessian Server will send a block notification to the Sender and the email will not be sent to the recipient.

If the Add-in or Gateway cannot connect to the Tessian Server or do not receive a response from the Tessian Server within the Default Threshold Period, the outgoing email will be sent to the recipient without any warning notification being presented to the Sender or any audit log being created.

Tessian Enforcer uses machine learning to detect anomalies in emails being sent. The email attributes which Tessian Enforcer identifies as anomalies are constantly evolving based on learning from users' sending behaviours. As a result, not all warning emails detected by Tessian Enforcer will be being sent to unauthorised recipients.

Tessian Defender

If an Authorised user issues an instruction to Customer's email system to send an email or receives an email, the following process will apply when Tessian Defender is in use: 1. The Tessian Server is called by the Add-in or Gateway. 2. The Tessian Server seeks to detect anomalies which may infer that the email may have been received from a suspicious sender. 3. If anomalies detected by the Tessian Server imply that the email has been received from a suspicious sender, the Tessian Server will generate a warning notification which will be presented to the Sender explaining the anomaly. Tessian Defender uses machine learning to detect anomalies in emails being received. Due to the predictive nature of the system, not all suspicious emails will be identified as such by Tessian Defender.

IMPORTANT NOTE: *Customers using Google GSuite with Comprehensive Mail Storage enabled should note that because of the way Google configures this service, Tessian Defender will not work and should not be used or relied on.*

Audit Logs

The Tessian Server creates audit logs of key events from the Tessian Platform, Tessian Guardian and Tessian Enforcer. Administrators may request a record of audit logs in a .CSV file format via the Tessian Server. In addition, Administrators may request a daily email notification from the Tessian Server giving them a snapshot of elements of the audit log data from the past 24-hour period.