DATA SECURITY EXHIBIT

1. **Introduction.** This Data Security 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. Unless defined herein, capitalized terms used in this Data Security Exhibit will have the meaning given to them in the Terms and Conditions.

2. **Hosting.** Tessian's database infrastructure is hosted on Amazon Web Services (AWS) (the "**Tessian Database**"). Tessian's databases are stored with Amazon Web Services in Ireland or the United States.

3. Tessian agrees to:
   a. ensure that each customer's Customer Data will be stored in a logically separated scheme when at rest in the Services;

   b. ensure that all API communication between Tessian hosted Software and the client-side environment uses TLS protocol to ensure Customer Data is encrypted in transit;

   c. encrypt all persisted Customer Data stored within the Tessian Database at rest;

   d. ensure all API calls are authenticated by a unique API token for each customer;

   e. require authenticated access to the Tessian web portal via unique usernames, and passwords, for every Administrator;

   f. ensure adequate physical and logical access control, using the following principles: need to know, least privilege, role-based access control, segregation of duties, and two-factor authentication methods;

   g. perform periodic reviews of access logs, user accounts and permissions;

   h. control all changes in Tessian organisation, business processes, information processing facilities and systems that affect information security (and changes should be planned, tested prior to implementation and have rollback options);

   i. test all new or changed Tessian information processing systems for functionality and security adequacy before implementation;

   j. implement a vulnerability management process to determine the need for updates and patches to Tessian information processing systems (these will be implemented in order to minimise the risks related to known vulnerabilities);

   k. use reasonable endeavours to detect and prevent information leakage and compromise through (for example) a non-exclusive combination of firewalls, HIDS, NIDS (which systems will be kept up-to-date);

   l. separate the Customer Data and of any type of backup of the Customer Data from any other data held by Tessian;

   m. before employing staff for roles involved with access to the Customer Data or to systems that might impact the security of the Customer Data, perform checks against candidates (e.g. verification of criminal record, competences) within the limits of applicable legislation;

n. provide regular security training to individuals working for or on behalf of Tessian with access to the Customer Data or to systems that might impact the security of the Customer Data; and

o. implement a due diligence process on third parties that are contracted by Tessian commensurate with the potential impact they might have on the security of the Customer Data.