Email Targeted Attack Protection | Proofpoint (General)

1. Definitions

In this section:

(a) **CASB** means Cloud App Security Broker;

(b) **DLP** means Data Loss Prevention**;**

(c) **DMARC** means Domain-based Message Authentication, Reporting and Conformance, an email authentication protocol designed to give email domain owners the ability to protect their domain from unauthorised use;

(d) **Licence(s)** means the licence metric (e.g., type and quantity) referenced in this Proposal;

(e) **Personal Data** means data which is 'personal information', as that term is defined in the *Privacy and Data Protection Act 2014* (Vic);

(f) **Proofpoint** means Proofpoint, Inc.;

(g) **Proofpoint Product(s)** means the appliances, services or software licensed and/or purchased by the Customer under this Proposal and includes DMARC, PSAT, CASB and DLP;

(h) **PSAT** means Proofpoint Security Awareness Training Enterprise Suite;

(i) **Threat Analytics** means information collected, generated and/or analysed by the Proofpoint Products, such as log files, statistics, aggregated data and derivatives thereof; and

(j) **User** means the Customer's employees, agents, subcontractors, consultants, or other individuals authorised by the Customer to use the Proofpoint Product.

2. Licence Count

(a) The Customer must monitor its actual usage of the subscription-based Proofpoint Products based on the Licences and must promptly inform Cenitex of the actual Licence count ("**Licence Count**"):

(1) if there is an increase in the Licence Count equal (or greater) than ten percent (10%) of the then current licensed Licence Count; or

(2) on request from Cenitex.

(b) Cenitex may also at any time provide a Licence Count to the Customer for verification by the Customer.

3. Use of Proofpoint Products

(a) The Customer's right to use the Proofpoint Products is limited to the maximum numbers of Licences, the deployment type (Appliance, Software or SaaS) for each module and any other limitations specified in this Proposal (including in this section).

(b) The Customer must ensure that each User is assigned a separate account on the Customer's email server for sending or receiving messages or data within the Customer's email system or network.

(c) The Customer must not:

(1) resell, sublicense, lease or otherwise make a Proofpoint Product available to any third party (except to subcontractors and subject to the rights set out in this clause 3;

(2) attempt to gain unauthorised access to, or disrupt the integrity or performance of, the Proofpoint Products or the data contained therein (including, but not limited to, penetration testing of Proofpoint's systems);

(3) modify, copy or create derivative works based on the Proofpoint Products;

(4) decompile, disassemble, reverse engineer or otherwise attempt to derive source code from the Proofpoint Products (in whole or part); or

(5) access a Proofpoint Product for the purpose of building a competitive product or service or copying its features or user interface.

(d) The Customer must not use a Proofpoint Product, or permit it to be used, for the purposes of:

(1) product evaluation, benchmarking or other comparative analysis intended from publication outside of the Customer's organisation without Proofpoint's prior written approval;

(2) infringement of the intellectual property rights of any third party or any rights of publicity or privacy;

(3) violation of any law, statute, ordinance, or regulation (including, but not limited to, the laws and regulations governing export/import control, unfair competition, anti-discrimination, and/or false advertising);

(4) propagation of any virus, worms, Trojan horses, or other programming routine intended to damage any system or data; and/or

(5) filing copyright or patent applications that include the Proofpoint Product and/or documentation or any portion thereof.

(e) The Customer must not use TAP Isolation products to monitor any User's internet activities and will not allow Users to transmit through or post on a TAP Isolation product infringing, defamatory, threatening or offensive material.

4. Provision of data

The Customer acknowledges and agrees that, in accessing or using the Proofpoint Products, it is giving Proofpoint the right to collect and process certain confidential information, Customer data and Personal Data from the Customer for the following purposes:

(a) abuse and threat awareness, detection and prevention;

(b) compliance; and

(c) security.

5. Threat Analytics

The Customer acknowledges and agrees that Proofpoint may collect Threat Analytics from the Customer, and may use the Threat Analytics to maintain, improve and enhance Proofpoint services.

6. DMARC

The Customer acknowledges and agrees that DMARC is for use with normal business messaging traffic only, and the Customer agrees that it shall not use DMARC for machine generated message delivery of bulk or unsolicited emails or emails sent from an account not assigned to an individual.

7. Hosting (PSAT)

The Customer acknowledges and agrees that PSAT Proofpoint Products will be hosted by AWS in Australia. The Closed-Loop Email Analysis and Response (CLEAR) integration between Proofpoint Threat Response Auto-Pull (TRAP) and Proofpoint PhishAlarm Analyzer (PAA) is hosted in the United States of America.

8. Hosting (CASB and DLP)

The Customer acknowledges and agrees that one or more CASB and/or Proofpoint Products will be hosted in Proofpoint's data centre in the Netherlands.