BUSINESS ASSOCIATE AGREEMENT

Can I Phish Pty Ltd — Standard Form

This Business Associate Agreement (this "BAA") is made between the parties identified below, with effect from the Effective Date.

Business Associate

Can I Phish Pty Ltd (ABN 24 647 802 266), an Australian proprietary limited company of PO Box 186, Peregian Beach, QLD 4573, Australia ("CanIPhish" or "Business Associate").

Covered Entity

Legal name: _____

Entity type and jurisdiction of organisation: _____

Address: _____

("Customer").

Effective Date: _____

CanIPhish and Customer are each a "Party" and together the "Parties".

BACKGROUND

A. Customer is either a "covered entity" or a "business associate" of a covered entity, as those terms are defined at 45 CFR § 160.103, and is required to comply with HIPAA in respect of Protected Health Information.

B. CanIPhish provides Customer with security awareness training, phishing simulation, phishing reporting and related security services under the Agreement. Those services are not health care services, do not involve the processing of health care transactions, and are neither designed nor intended to receive Protected Health Information.

C. Notwithstanding paragraph B, members of Customer's workforce may, by using the reporting features of the Services, submit email messages to CanIPhish that incidentally contain Protected Health Information.

D. The Parties enter into this BAA to satisfy the requirements of 45 CFR §§ 164.502(e), 164.504(e) and 164.308(b) in respect of any such Protected Health Information, and to record the scope and limits of each Party's obligations.

The Parties agree as follows.

1. DEFINITIONS

1.1 Capitalised terms used but not defined in this BAA have the meanings given to them in HIPAA. In this BAA:

- **"Agreement"** means the CanIPhish Terms & Conditions available at https://caniphish.com/terms-conditions and the CanIPhish Subscription & Service Level Agreement available at https://caniphish.com/Supporting/CanIPhish-Subscription-And-Service-Level-Agreement.pdf (in each case, or their successors), together with each order form, subscription or quote under which CanIPhish provides the Services to Customer.
- **"Breach"** has the meaning given at 45 CFR § 164.402.
- **"Breach Notification Rule"** means Subpart D of 45 CFR Part 164.
- **"Designated Record Set"** has the meaning given at 45 CFR § 164.501.
- **"Discovery"** has the meaning given at 45 CFR § 164.410(a)(2).
- **"Electronic PHI" or "ePHI"** means PHI maintained in or transmitted by electronic media, as defined at 45 CFR § 160.103.
- **"HHS"** means the United States Department of Health and Human Services, and includes its Office for Civil Rights.
- **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191), as amended by the HITECH Act, together with the regulations promulgated by HHS thereunder, each as amended from time to time.
- **"HITECH Act"** means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5).
- **"Individual"** has the meaning given at 45 CFR § 160.103 and includes a personal representative in accordance with 45 CFR § 164.502(g).
- **"Privacy Rule"** means 45 CFR Part 160 and Subparts A and E of 45 CFR Part 164.
- **"Protected Health Information" or "PHI"** has the meaning given at 45 CFR § 160.103, limited to information created, received, maintained or transmitted by CanIPhish from or on behalf of Customer in connection with the Services.
- **"Reported Message"** means an email message, including its headers, body content and attachments, that a member of Customer's workforce submits to the Services using a reporting add-in, integration, connector or reporting mailbox.
- **"Required by Law"** has the meaning given at 45 CFR § 164.103.
- **"Security Incident"** has the meaning given at 45 CFR § 164.304, as qualified by Section 6.3 of this BAA.
- **"Security Rule"** means 45 CFR Part 160 and Subparts A and C of 45 CFR Part 164.
- **"Services"** means the products and services made available by CanIPhish to Customer under the Agreement.
- **"Subcontractor"** has the meaning given at 45 CFR § 160.103.
- **"Unsecured PHI"** has the meaning given at 45 CFR § 164.402.

2. SCOPE AND NATURE OF THE SERVICES

2.1 No PHI required. The Services do not require access to PHI. CanIPhish does not provide health care, process health care transactions, or perform any function or activity on Customer's behalf that requires the use or disclosure of PHI.

2.2 Incidental receipt only. CanIPhish may receive PHI only incidentally, as a consequence of Customer's workforce submitting Reported Messages that happen to contain PHI. The Parties acknowledge that such submissions are initiated by Customer's own workforce and that the content of Reported Messages is not selected, requested or controlled by CanIPhish.

2.3 Minimisation by Customer. Customer will configure the Services, and will instruct and train its workforce, so as to minimise the PHI transmitted to CanIPhish. Customer will not intentionally use the Services to transmit, store or process PHI. Customer is responsible for electing any configuration CanIPhish makes available that limits the retention or processing of Reported Message content, including the Subcontractor restrictions described in Section 5.3.

2.4 No Designated Record Set. CanIPhish does not create, receive, maintain or transmit PHI in a Designated Record Set on Customer's behalf. Section 9 applies only if and to the extent that this position changes and the Parties agree in writing that CanIPhish maintains PHI in a Designated Record Set.

2.5 Data not covered. This BAA applies only to PHI. It does not apply to any other Customer data processed under the Agreement, including simulation results, training and assessment records, employee and target lists, authentication data, usage telemetry, or billing information, all of which are governed by the Agreement and CanIPhish's privacy policy.

3. PERMITTED USES AND DISCLOSURES OF PHI

3.1 General. CanIPhish will not use or disclose PHI other than as permitted or required by this BAA, as permitted by the Privacy Rule, or as Required by Law. CanIPhish will not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by Customer, except as permitted by Sections 3.2 and 3.3.

3.2 Management and administration. CanIPhish may use PHI in its possession for its proper management and administration and to carry out its legal responsibilities. CanIPhish may disclose PHI for those purposes only where (a) the disclosure is Required by Law, or (b) CanIPhish obtains, in writing and in advance, reasonable assurances from the recipient that the PHI will be held confidentially and used or further disclosed only as Required by Law or for the purpose for which it was disclosed, and that the recipient will notify CanIPhish of any breach of confidentiality of which it becomes aware.

3.3 De-identification and aggregation. Customer authorises CanIPhish to de-identify PHI in accordance with 45 CFR §§ 164.514(a) and (b), and to provide data aggregation services relating to Customer's health care operations as permitted by 45 CFR § 164.504(e)(2)(i)(B). Information de-identified in accordance with 45 CFR § 164.514 is not PHI, is not subject to this BAA, and may be used and disclosed by CanIPhish for any lawful purpose, including operating, securing and improving the Services.

3.4 Minimum necessary. CanIPhish will, to the extent practicable, limit its use, disclosure of and request for PHI to a limited data set or, where that is not practicable, to the minimum necessary to accomplish the intended purpose, consistent with 45 CFR § 164.502(b) and section 13405(b) of the HITECH Act.

3.5 Reporting unlawful conduct. CanIPhish may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 CFR § 164.502(j)(1).

3.6 Prohibited uses. CanIPhish will not (a) directly or indirectly receive remuneration in exchange for PHI except as permitted by 45 CFR § 164.502(a)(5)(ii), or (b) make or cause to be made any communication about a product or service that would be prohibited by 45 CFR §§ 164.501 and 164.508(a)(3).

4. SAFEGUARDS

4.1 CanIPhish will use appropriate safeguards, and will comply with Subpart C of 45 CFR Part 164 with respect to ePHI, to prevent the use or disclosure of PHI other than as permitted by this BAA. CanIPhish will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the ePHI it creates, receives, maintains or transmits on behalf of Customer.

4.2 Without limiting Section 4.1, CanIPhish maintains:

(a) encryption of ePHI in transit over public networks and at rest;

(b) role-based access controls applying the principle of least privilege, and logging of personnel access to Reported Message content;

(c) a documented risk analysis and risk management process;

(d) security awareness training for its workforce, written confidentiality obligations, and a sanction policy for workforce members who fail to comply with its security policies; and

(e) documented incident response, backup and contingency plans.

4.3 A current description of CanIPhish's technical and organisational security measures is available at https://caniphish.com/security and in Annex II of the CanIPhish Data Processing Agreement. CanIPhish may modify its safeguards from time to time provided it does not materially reduce the level of protection afforded to PHI.

5. SUBCONTRACTORS

5.1 In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), CanIPhish will ensure that any Subcontractor that creates, receives, maintains or transmits PHI on its behalf agrees in writing to restrictions and conditions that are at least as protective as those in this BAA, and to comply with the applicable requirements of the Security Rule.

5.2 A current list of Subcontractors is set out in Annex III of the CanIPhish Data Processing Agreement, available at https://caniphish.com/Supporting/Data-Processing-Agreement-CanIPhish.pdf. CanIPhish will give Customer at least thirty (30) days' notice before engaging

a new Subcontractor with access to PHI. If Customer reasonably objects on the ground that the Subcontractor cannot meet the requirements of Section 5.1, and CanIPhish cannot provide the Services without that Subcontractor, either Party may terminate the affected Services on written notice.

5.3 Customer-managed Subcontractor restrictions. CanIPhish makes available Privacy Settings through which Customer may disable individual non-essential Subcontractors. The ability to change these settings is a feature of CanIPhish's Enterprise plan; on other plans Customer may review its Subcontractors and their data locations but cannot change them. Disabling a Subcontractor also disables the platform functionality that Subcontractor powers; in particular, disabling the AI Subcontractor disables AI threat analysis of reported email. Amazon Web Services provides CanIPhish's core hosting and storage and cannot be disabled. Disabling a Subcontractor prevents further data being sent to it but does not retroactively affect data already processed, so Customer should elect its configuration before enabling any reporting feature. Customer is responsible for selecting and maintaining the configuration appropriate to its obligations under HIPAA. Current documentation is available at https://help.caniphish.com/hc/en-us/articles/16847617669135-Privacy-Settings-Subprocessor-Management-Introduction.

5.4 CanIPhish remains responsible to Customer for the performance of its Subcontractors under this BAA.

6. REPORTING OF IMPERMISSIBLE USES AND SECURITY INCIDENTS

6.1 CanIPhish will report to Customer, without unreasonable delay, any use or disclosure of PHI not permitted by this BAA of which it becomes aware.

6.2 CanIPhish will report to Customer any Security Incident affecting ePHI of which it becomes aware, without unreasonable delay and in any event within thirty (30) business days of becoming aware of it.

6.3 Unsuccessful attempts. The Parties acknowledge that CanIPhish operates internet-facing systems that are subject to a continuous and substantial volume of unsuccessful attempts to access, use, disclose, modify or destroy information, or to interfere with system operations, including pings and other broadcast attacks, port scans, unsuccessful log-on attempts, denial of service attempts, malformed packets, and traffic blocked or filtered by network controls. The Parties agree that individual reporting of such unsuccessful attempts would be of no practical value to Customer. This Section 6.3 constitutes notice by CanIPhish, and acknowledgement by Customer, that such unsuccessful attempts occur on an ongoing basis, and no further report of them is required unless and until an attempt results in unauthorised access to, or the unauthorised use, disclosure, modification or destruction of, ePHI.

7. BREACH NOTIFICATION

7.1 CanIPhish will notify Customer in writing of any Breach of Unsecured PHI in accordance with 45 CFR § 164.410, without unreasonable delay and in no case later than thirty (30) calendar days after Discovery of the Breach.

7.2 The notification will include, to the extent known at the time and updated as further information becomes available: the identification of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed; a description of what occurred; the date of the Breach and the date of Discovery; the types of PHI involved; the steps CanIPhish has taken to investigate and mitigate the Breach; and a contact point for further information.

7.3 Customer is solely responsible for determining whether a Breach requires notification to Individuals, HHS, the media or any other party, and for making any such notification, unless the Parties agree otherwise in writing.

7.4 Any obligation of CanIPhish to reimburse Customer for costs arising from a Breach, whether under this BAA or otherwise, is subject to and counts toward the limitations of liability set out in the Agreement.

8. MITIGATION

8.1 CanIPhish will take reasonable measures to mitigate, to the extent practicable, any harmful effect known to it of a use or disclosure of PHI by CanIPhish or its Subcontractors in violation of this BAA.

9. INDIVIDUAL RIGHTS

9.1 This Section 9 is subject to Section 2.4. If and to the extent CanIPhish maintains PHI in a Designated Record Set on Customer's behalf, CanIPhish will, within fifteen (15) business days of Customer's written request, (a) make that PHI available to Customer so that Customer can meet its obligations under 45 CFR § 164.524, and (b) make any amendment to that PHI directed by Customer in accordance with 45 CFR § 164.526.

9.2 If CanIPhish receives a request for access to, amendment of, or an accounting of disclosures of PHI directly from an Individual, it will forward that request to Customer within ten (10) business days. Any decision to grant or deny such a request, and any response to the Individual, is the sole responsibility of Customer.

9.3 CanIPhish will document disclosures of PHI, and information relating to those disclosures, as would be required for Customer to respond to a request for an accounting of disclosures under 45 CFR § 164.528, and will provide that documentation to Customer within twenty (20) business days of written request.

10. AVAILABILITY OF RECORDS TO HHS

10.1 CanIPhish will make its internal practices, books and records relating to the use and disclosure of Customer's PHI available to the Secretary of HHS for purposes of determining Customer's or CanIPhish's compliance with HIPAA.

10.2 To the extent legally permitted, CanIPhish will notify Customer of any such request before responding, and will disclose only that information reasonably required. This Section 10 does not confer any audit or inspection right on Customer.

11. SECURITY ASSURANCE

11.1 CanIPhish maintains an annual SOC 2 Type II examination of its security controls. On written request, and no more than once in any twelve (12) month period, CanIPhish will provide Customer with a copy of its most recent SOC 2 Type II report, subject to Customer first executing a non-disclosure agreement where CanIPhish reasonably requires one.

11.2 If CanIPhish ceases to maintain such a report, it will instead complete a reasonable written security questionnaire, no more than once in any twelve (12) month period. Customer may make one additional request under Section 11.1 or 11.2 following a Breach affecting Customer's PHI.

11.3 Sections 11.1 and 11.2 state Customer's sole assurance rights under this BAA. Customer has no right to conduct an on-site inspection, audit, vulnerability scan or penetration test of CanIPhish's systems except with CanIPhish's prior written agreement and on terms to be agreed.

12. OBLIGATIONS OF CUSTOMER

12.1 Customer will notify CanIPhish of (a) any limitation in its notice of privacy practices under 45 CFR § 164.520, (b) any change in, or revocation of, an Individual's permission to use or disclose PHI, and (c) any restriction on the use or disclosure of PHI that Customer has agreed to or must abide by under 45 CFR § 164.522, in each case to the extent it may affect CanIPhish's use or disclosure of PHI.

12.2 Customer will not request CanIPhish to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Customer, except as permitted by Sections 3.2 and 3.3.

12.3 Customer will comply with Section 2.3 and will not transmit PHI to CanIPhish other than incidentally through Reported Messages.

12.4 Customer represents and warrants that it has obtained all consents, authorisations and permissions necessary for PHI to be disclosed to CanIPhish and used by CanIPhish as contemplated by this BAA and the Agreement.

13. DATA OWNERSHIP

13.1 CanIPhish's stewardship of PHI under this BAA does not confer on CanIPhish any ownership right in that PHI.

14. TERM AND TERMINATION

14.1 This BAA takes effect on the Effective Date and continues until the Agreement terminates or expires and all obligations of the Parties under this BAA have been discharged.

14.2 Either Party may terminate this BAA and the Agreement if it determines that the other Party has materially breached this BAA and the breaching Party has failed to cure that breach to the terminating Party's reasonable satisfaction within thirty (30) days of written notice. If cure is not possible and termination is not feasible, the non-breaching Party may report the matter to HHS.

14.3 On termination of this BAA or the Agreement for any reason, CanIPhish will return to Customer or destroy all PHI it maintains on Customer's behalf, and will retain no copies, except as provided in Section 14.4. This obligation extends to PHI in the possession of CanIPhish's Subcontractors. If return or destruction is infeasible in CanIPhish's reasonable judgement, CanIPhish will notify Customer in writing of the conditions making it infeasible, will extend the protections of this BAA to that PHI for so long as it retains it, and will limit further uses and disclosures to those purposes that make return or destruction infeasible.

14.4 Backups and archives. The Parties acknowledge that PHI may persist in routine system backups, immutable archives, replication snapshots and audit or security logs from which individual records cannot be selectively deleted without disproportionate effort or without compromising the integrity of those records. Such PHI is exempt from Section 14.3, provided that CanIPhish (a) makes no further use or disclosure of it other than as necessary for backup, restoration, security or legal-hold purposes, (b) continues to protect it in accordance with this BAA for so long as it is retained, and (c) destroys it in the ordinary course of its documented backup rotation and retention schedule.

14.5 Sections 3, 4, 7, 10, 13, 14.3, 14.4, 15 and 17 survive termination of this BAA for so long as CanIPhish retains any PHI.

15. RELATIONSHIP TO THE AGREEMENT

15.1 This BAA supplements and forms part of the Agreement.

15.2 If there is a conflict between this BAA and the Agreement with respect to the use, disclosure or safeguarding of PHI, this BAA governs. In all other respects the Agreement governs.

15.3 The provisions of the Agreement relating to limitation of liability, exclusion of indirect and consequential damages, governing law, jurisdiction and venue, and dispute resolution apply to this BAA as if set out in it, and are not modified, expanded or waived by this BAA.

15.4 Any ambiguity in this BAA is to be resolved in favour of a meaning that permits compliance with HIPAA.

15.5 Nothing in this BAA requires CanIPhish to comply with any security standard, control framework, certification or state law that does not apply to it as a business associate under HIPAA, except as separately agreed in writing.

15.6 This BAA does not create any rights in favour of any third party.

16. CHANGES IN LAW

16.1 A reference in this BAA to a section of HIPAA is to that section as in effect or as amended at the relevant time.

16.2 The Parties will negotiate in good faith to amend this BAA as reasonably necessary to comply with amendments to HIPAA. If the Parties are unable to agree an amendment within thirty (30) days of a Party requesting one, either Party may terminate this BAA and the Agreement on thirty (30) days' written notice.

16.3 If an amendment to HIPAA materially increases CanIPhish's cost of performing under this BAA, CanIPhish may adjust its fees with effect from the next renewal term on sixty (60) days' written notice, and Customer may elect not to renew.

17. GENERAL

17.1 Amendment and waiver. This BAA may only be amended in writing signed by authorised representatives of both Parties. A waiver in respect of one event is not a continuing waiver or a waiver in respect of any other event.

17.2 Notices. Notices under this BAA must be given by registered post, express courier or email to:

(a) CanIPhish: Can I Phish Pty Ltd, PO Box 186, Peregian Beach, QLD 4573, Australia, Attention: Legal, email support@caniphish.com.

(b) Customer: the address and email set out beneath Customer's signature below, or as notified in writing.

17.3 Counterparts and electronic signature. This BAA may be executed in counterparts and by electronic signature, each of which is an original and all of which together constitute one agreement.

17.4 Severability. If any provision of this BAA is held invalid or unenforceable, the remainder continues in full force and effect.

17.5 Entire agreement. This BAA, together with the Agreement, is the entire agreement between the Parties in respect of PHI and supersedes any prior understanding on that subject.

The Parties have executed this BAA as of the Effective Date.

CAN I PHISH PTY LTD (ABN 24 647 802 266)

Signature: _____

Name: _____

Title: _____

Date: _____

CUSTOMER

Signature: _____

Name: _____

Title: _____

Date: _____

Notice address: _____

Notice email: _____