APM Consulting Agreement

CompanyCam ("Client") and The Speedshop Kabushiki Kaisha ("Speedshop" and collectively the "Parties" and individually as a "Party") enter into this APM Consulting Agreement (the "Agreement") as follows:

Article 1 (Purpose)

Client requires consulting services related to application performance issues as described in Article 2 of this Agreement (the "Services") of the CompanyCam web and mobile application coded with Ruby on Rails (the "Application") and Speedshop agrees to provide the Services in accordance with this Agreement.

Article 2 (Services)

1. The contents of the Services are as follows and Speedshop shall implement the Services subject to the terms and conditions in this Agreement:
   (1) to set up automated alerts, monitors, and dashboards for the Application in Client's system;
   (2) to attempt to fix small Application's performance issues that can be fixed within one day according to Client's request;
   (3) to review and give feedbacks on Application's performance related changes contemplated by Client;
   (4) to respond to inquiries concerning Application's performance issues via telephone or chat; and
   (5) to provide a monthly report on the Application's performance.
2. Any services requested by Client which are not listed in the preceding paragraphs are not included in the Services and may be performed by Speedshop for a fee pursuant to an amendment to this Agreement separately agreed to in writing and duly executed by both Parties.

Article 3 (Implementation and Time)

1. Speedshop will provide all of the Services remotely to Clients.

Article 4 (Fees)

1. Client shall pay 2,400 US Dollars per month (exclusive of consumption tax) to Speedshop as consideration for the Services (the "Fees").
2. The Fees and Expenses (as defined in Article 5) shall be paid by telegraphic transfer to a bank account designated by Speedshop within 15th day of Client's receipt of invoice issued by Speedshop. Remittance fees shall be borne by Client.
3. Client will have 15 days after receipt of an invoice to dispute the amount of the invoice by providing written notice to Speedshop (e.g., via email). Client and Speedshop shall work in good faith to resolve any disputed invoices. Such disputed invoices shall not be subject to Article 6.

Article 5 (Costs)

Client shall reimburse all Client pre-authorized out-of-pocket expenses incurred by Speedshop in connection with performing the Services("Expenses").

Article 6 (Delay Damages)

If Client does not fulfill its payment obligations (excluding disputed payments as described in paragraph 3 of Article 4, if any) on the payment due date as stipulated in paragraph 2 Article 4, 1% of the amount of the late payment due shall accrue as the delay damages, calculated from the day after the payment date until the completion of the full payment.

Article 7 (Obligations)

1. In connection with the performance of the Services, Client shall provide Speedshop with all such cooperation and assistance as Speedshop reasonably requests, or

otherwise may reasonably be required, to enable Speedshop to perform its obligations (including the provision of the Services) under and in accordance with the terms and conditions of this Agreement.

2. If any materials, information or data (collectively "Materials") are necessary for the performance of the Services, Speedshop may request Client to provide such Materials and Client shall provide such Materials without delay to Speedshop.
3. Client agrees to back up all data, files, and information prior to the performance of any Services and hereby assumes sole responsibility for any lost or altered data, files, or information unless such loss or altered data, files, or information was caused by the acts or omissions of Speedshop or its employees, contractors, agents, or representatives.

Article 8 (Subcontracting)

Speedshop may subcontract any part or all of the Services to a third party as Speedshop deems necessary for the performance of the Services, provided, however, that Speedshop shall enter into a binding written agreement with any third party that ensures that such third party fully complies with the terms and conditions set forth in this Agreement including, but not limited to, the provision of the Agreement governing Confidential Information. Speedshop assumes all responsibility and liability for the actions any such third party.

Article 9 (Intellectual Property Ownership and Data Protection)

1. Client is and will remain the sole and exclusive owner of all rights, title, and interest in and to any documents, data, know-how, specifications, methodologies, software, and any other materials owned and/or licensed by Client and provided to Speedshop for use in connection with the Services, including all Intellectual Property Rights. This includes all data provided by Client or generated through the performance of the Services.

   1. For purposes of this Agreement, "Intellectual Property Rights" means on a worldwide basis any (a) copyrights, moral rights, mask works, rights of authorship, and all derivatives; (b) trade secret, know-how, or other confidential or proprietary information rights; (c) patents and any continuations, continuations-in-part, divisionals, extensions, substitutions, reissues, re-examinations, and renewals; (d) trademarks, trade name rights, service marks, names, logos, rights of publicity, and similar rights and associated goodwill; (e) intellectual and industrial property rights (of every kind and nature throughout the world and however designated); and (f) the Application and any other applications, registrations, or common law rights in any of the foregoing, as applicable.
   2.
2. Speedshop irrevocably assigns to Client all right, title and interest worldwide in and to any CompanyCam Content and all Intellectual Property Rights in any CompanyCam Content. Speedshop retains no rights in the CompanyCam Content and agrees not to challenge the validity of Client's ownership of the CompanyCam Content.

   For the purposes of this Agreement, "CompanyCam Content" means any ideas, concepts, processes, discoveries, developments, information, materials, improvements, designs, artwork, content, software programs, other copyrightable works, and any other work product created, conceived or developed by Speedshop (whether alone or jointly with others) for Client in performing the Services.
   3.
3. **In performing the Services, Speedshop, its employees and subcontractors may be required to Process CompanyCam Data. The Parties agree to comply with the terms of the Data Processing Addendum ("DPA") which is attached as Exhibit A and incorporated by reference with respect to the processing of such CompanyCam Data.**

Article 10 (Confidentiality)

1. Neither Party shall disclose or divulge to a third party any information of the other Party ("Disclosing Party"), including but not limited to nonpublic business or technical

information, trade secrets, or information or data that Disclosing Party designates to be of a confidential natures or should be reasonably known to the other Party ("Receiving Party") to be confidential due to the nature of the information and the circumstances surrounding the disclosure.("Confidential Information"), without the prior written consent of the other Party. For the avoidance of doubt, Materials are included in Client's Confidential Information. The Parties shall use Confidential Information solely for the performance of the Services and shall not use it for any purpose. Confidential Information shall not be disclosed by the Receiving Party to any third party by any way including but not limited to in writing, orally, or through electro-magnetic media. The Receiving Party shall treat all Confidential Information of the Disclosing Party in accordance with this Article 10 in perpetuity, unless such information is released into the public domain by the Disclosing Party.

2. Notwithstanding the preceding paragraph 1 of this Article 10, the following items do not fall under Confidential Information:
   (a) information that is in the public domain at the time of the disclosure;
   (b) the Receiving Party can demonstrate that the information was already in possession of the recipient at the time of the disclosure;
   (c) information that enters into the public domain for reasons not attributable to the Receiving Party after the disclosure;
   (d) the Receiving Party can demonstrate that the information lawfully obtained from a third party without any obligation of confidentiality; or
   (e) the Receiving Party can demonstrate that the information was independently developed without reference to Confidential Information of other party.
4. Notwithstanding paragraph 1 of this Article 9, Speedshop may disclose Confidential Information without the prior written consent of Client in any of the following events:
   (a) Speedshop may disclose Confidential Information to its officers or employees or to its affiliates, or experts such as lawyers, accountants, or tax accountants within the scope necessary for the performance of the Services; provided that the person to whom the disclosure is to be made is held to at least the same confidentiality obligations as those set forth in this Agreement in accordance with any applicable laws, regulations, or other agreements where it is a party; and
   (b) if Speedshop is required or requested to disclose Confidential Information by the government, any competent authorities, regulatory authorities, courts, or financial instruments exchange pursuant to applicable laws and regulations (including the rules of financial instruments exchanges), Speedshop may disclose Confidential Information, provided that Speedshop shall promptly notify Client in writing of the content of such disclosure in advance and given an opportunity to obtain a suitable protective order (in the event such notification in advance is not permissible by law, as soon as possible after such disclosure).

Article 11 (Compensation for Damage)

1. If a Party is obliged to pay damages, regardless of the legal grounds, including liability for non-performance, tort, statutory liabilities, or attorneys' fee to the other Party in connection with this Agreement, such Party shall compensate the other Party only for direct and actual damages.
2. Except in the case of gross negligence or willful misconduct, infringement of Intellectual Property Rights, in no event shall either party's liability to the other or any third party exceed the amount of one year's worth of Fees.

Article 12 (Force Majeure)

1. Force Majeure means, in this Agreement, circumstances beyond its reasonable control, and which it could not have mitigated, avoided, or prevented, including, without limitation, earthquake, typhoon, tsunami and other acts of God, wars, civil disturbances, riot, acts of terrorism, unexpected accident, strike, lockout, occurrence of serious disease or infectious disease, change in laws or regulations, and acts of any governmental body.
2. Neither Party shall be liable for any failure of or delay in performance of its obligation

under this Agreement, to the extent such failure or delay is due to Force Majeure.

Article 13 (Termination for Cause)

1. Either Party may unilaterally terminate this Agreement if the other Party materially breaches any provision of this Agreement and does not cure such breach within 30 days of written notice of such material breach.
2. Either Party may unilaterally terminate all or a part of this Agreement immediately without prior written notice to the other Party if any of the following events applies to the other Party (unless such event is attributable to the terminating Party):
   (a) if the other Party commits any material breach of this Agreement or is in breach of good faith;
   (b) if the other Party becomes subject of a voluntary or involuntary bankruptcy procedure, civil rehabilitation procedure, corporate reorganization procedure, or any other liquidation procedure;
   (c) if the other Party becomes insolvent; or
   (d) if the other Party dissolves itself or abolishes its businesses.
3. If Client terminates this Agreement in accordance with paragraph 1 or 2 of this Article 13, the Client's payment obligations for earned Services under this Agreement will be accelerated and become immediately due and payable. If Speedshop terminates this Agreement in accordance with paragraph 1 or 2 of this Article 13, Speedshop shall immediately refund Client all prepaid Fees.
4. Termination as set forth in paragraph 1 or 2 of this Article 12 will not preclude the terminating Party from making a claim for damages against the other Party.

Article 14 (Term)

1. The term of this Agreement is for 6 months from May 1st 2025 until October 31, 2025.
2. Notwithstanding paragraph 1 of this Article 14, unless either Party notifies the other Party in writing of its intention to amend or terminate this Agreement no later than 1 months before the expiration date, this Agreement will be automatically renewed for 6 months, and the same terms and conditions will apply to other subsequent renewals.

Article 15 (Prohibition of Assignment)

Neither Party may assign any of the rights or delegate any of its obligations under this Agreement without obtaining the prior written consent of the other Party, which consent shall not be unreasonably withheld, conditioned, or delayed. Notwithstanding the previous limitations, either Party may assign its rights or delegate its obligations under this Agreement, in whole, but not in part, without such consent to (a) an affiliate, or (b) an entity that acquires all or substantially all of the business or assets of such Party, whether by merger, reorganization, acquisition, sale, or otherwise. Any purported assignment or delegation in violation of this provision will be null and void.

Article 16 (Entire Agreement)

This Agreement constitutes the entire agreement between the Parties regarding the subject matter of this Agreement and merges and supersedes all previous discussion, negotiationsand agreements, either oral or written, with respect to the subject matter hereof, and no addition to or modification of this Agreement shall be binding on either Party hereto unless reduced to writing and agreed upon by each of the Parties hereto.

Article 17 (Governing Law)

1. This Agreement will be governed by and construed in accordance with the laws of the State of Delaware.

Article 18 (Survival)

The provisions of Article 11 (Compensation for Damage), Article 12 (Force Majeure), paragraph 3 and 4 of Article 13 (Termination for Cause), Article 15 (Prohibition of Assignment), Article 16 (Entire Agreement), Article 17 (Governing Law and Jurisdiction), and this Article 18 (Survival) will survive the termination of this Agreement and will remain in full force and effect after the termination of this Agreement.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed and each Party shall retain one (1) copy each, duly signed and sealed by each Party, respectively.

May 1, 2025.

Client:

Address: 300 Canopy Street, Suite 200, Lincoln NE 68508

Entity name: CompanyCam, Inc.

Title and Name of Representative: Kevin Scully, SVP Engineering

Speedshop

1-1-30-1 Hamatake, Chigasaki, Japan, 253-0021
The Speedshop KK
Nathan Berkopec, Director

EXHIBIT A

DATA PROCESSING ADDENDUM

May 1 2025

This Data Processing Addendum ("**DPA**") is made as of the [DAY] day of [MONTH],2025 ("**Effective Date**"), between CompanyCam, Inc., a Delaware company, and Speedshop Kabushiki Kaisha (**"Service Provider"**) a Japanese company with offices at 1-1-30-1 Hamatake, Chigasaki, Japan, 253-0021. CompanyCam and Service Provider are each a "**Party**" and collectively the "**Parties**" to this DPA.

RECITALS

- CompanyCam and Service Provider are parties to an agreement effective as of May 1 2025 [EFFECTIVE DATE] (**"Agreement"**);
- In connection with performing the Services under the Agreement, Service Provider may have access to certain CompanyCam Data which is subject to regulation under applicable Data Protection Laws; and
- CompanyCam and Service Provider wish to enter into this DPA to address their respective obligations when Processing CompanyCam Data under the Agreement.

TERMS

NOW THEREFORE, for good and valuable consideration, the Parties agree as follows:

1. **Definitions.** Capitalized terms set forth in this DPA have the following meanings:

1.1. **"Affiliate(s)"** has the meaning set forth in the Agreement.

1.2. **"CompanyCam Data"** means any data or information Processed by Service Provider on behalf of CompanyCam, pursuant to the Agreement, including Personal Information.

1.3. **"Controller "** means the person or entity who determines the purposes and means of the Processing of Personal Information and includes the term "Business" as similarly defined under applicable Data Protection Laws.

1.4. **"Data Protection Laws"** means any applicable current and future laws, rules, regulations and guidance governing the privacy, security and protection of Personal Information processed under the Agreement, including but not limited to the US Data Protection Laws and the European Data Protection Laws.

1.5. **"Data Subject"** means an identified or identifiable natural person or a "Consumer" as defined under applicable Data Protection Laws.

1.6. **"European Data Protection Laws"** means all applicable legislation applicable to data protection and privacy regarding residents of the EU, UK or Switzerland, including but not limited to: (i) the EU General Data Protection Regulation ((EU) 2016/679) (the "EU GDPR"); (ii) Directive 2002/58/EC the Privacy and Electronic Communications Regulations 2003 as amended (iii) the EU GDPR as applicable as part of UK domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (as amended) ("UK GDPR"); (d) the Swiss Federal Act on Data Protection of 1 September 2023 and its corresponding ordinances (the "FADP"); and any applicable guidance or codes of practice issued by any applicable Supervisory Authorities from time to time.

1.7. **"IT Infrastructure"** means the information technology infrastructure owned or operated by or on behalf of CompanyCam, which includes certain hardware,

software, networks, communication systems, architecture, equipment, electronic devices, and data.

1.8. **"Personal Information " or "Personal Data"** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Consumer or household, or is otherwise regulated by applicable Data Protection Laws.

1.9. **"Personnel"** means those employees, Affiliates, approved agents, Service Providers or Sub-Processors that Service Provider uses to perform its obligations or exercise its rights under the Agreement or this DPA.

1.10. **"Process" or "Processing"** means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11. **"Service Provider"** means the entity that Processes Personal Information on behalf of CompanyCam and includes the term "Service Provider" as similarly defined under applicable Data Protection Laws.

1.12. **"Restricted Transfer"** means (i) where EU GDPR or the FADP applies, a transfer of Personal Information from the European Economic Area ("EEA") including Switzerland to a country outside of the EEA, which is not the subject of an adequacy determination by the European Commission; and (ii) where UK GDPR applies, a transfer of Personal Information from the United Kingdom to any country which is not subject based on adequacy regulations pursuant to Section 17A of the UK Data Protection Act.

1.13. **"Rights Request"** means a request from an individual seeking to exercise the rights granted to Data Subjects under the Data Protection Laws which may include, the right to access, correct, opt out, restrict Processing, data portability, delete or not to be subject to automated individual decision making.

1.14. **"Security Incident"** means unauthorized loss, destruction, acquisition, use, disclosure of, or access to CompanyCam Data in Service Provider's possession, custody, or control, or any other event that compromises the security, confidentiality or integrity of CompanyCam Data or CompanyCam's IT Infrastructure.

1.15. "**Security Program"** means a written comprehensive data privacy program which contains administrative, technical, and physical safeguards, policies, and procedures consistent with applicable Data Protection Laws.

1.16. **"Services"** has the meaning set forth in the Agreement.

1.17. **"Standard Contractual Clauses"** means:

in respect of Personal Data subject to GDPR, the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, including the text from Module Two and Module Three;

in respect of Swiss Personal Data, the EU Standard Contractual Clauses, provided that any references in the clauses to the GDPR shall refer to the FADP; the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses and

in respect of UK Personal Data, the International Data Transfer Addendum to

the EU Standard Contractual Clauses, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 but, as permitted by Clause 17 of such Addendum, the parties agree to change the format of the information set out in Part 1 of the Addendum so that:

i. The details of the parties in Table 1 of the Addendum shall be as set out in Appendix 1 to this DPA (with no requirement for signature);

ii. For the purposes of Table 2 of the Addendum, the Addendum shall be appended to the EU Standard Contractual Clauses (including the selection of modules and disapplication of optional clauses as noted above) and Clause 13(2)(a) below selects the option and timescales for Clause 9 of the EU Standard Contractual Clauses;

iii. The appendix information listed in Table 2 of the Addendum is set out in Appendices 2 and 3 to this DPA; and

iv. For the purposes of Table 3 of the Addendum, the following option is selected regarding which party/ies may end the Addendum as set out in Clause 19 thereof: the Data Controller only.

1.18. **"Sub-Processor"** means a third party engaged by Service Provider or another Service Provider to assist in the performance of the Services and which will Process CompanyCam Data.

1.19. **"Supervisory Authority"** means any international, federal, state, or local agency, department, official, legislature, or any governmental or professional body, regulatory or supervisory authority, board, or other body responsible for administration of and enforcement of the Data Protection Laws with regard to CompanyCam Data Processed under this Agreement.

1.20. **"US Data Protection Laws"** means the US federal, state and local laws, rules, regulations and guidance related to the privacy, security and protection of Personal Information processed under the Agreement, including but not limited to: (i) the Federal Trade Commission Act, 15 U.S.C. § 45 and its implementing regulations; (ii) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 and its implementing regulations, (iii) the Texas Data Privacy and Security Act, (iv) the Nebraska Data Privacy Act, and (v) any other federal or state consumer privacy laws, data breach notification laws and data security laws governing the protection of Personal Information.

2. Data Protection Obligations

2.1. **Roles of the Parties**. Where CompanyCam is a Business or Controller, Service Provider is a Processor within the meaning of the Data Protection Laws. Where CompanyCam is a Processor, Service Provider is a Sub-Processor. Service Provider may only Process CompanyCam Data for the business purposes specified in the Agreement.

2.2. **Compliance with Data Protection Laws**. Service Provider will have access to CompanyCam Data when performing the Services under the Agreement. Service Provider shall comply with all applicable Data Protection Laws when performing the Services and Processing CompanyCam Data. Service Provider will promptly inform CompanyCam if it is no longer able to meet its obligations under the Data Protection Laws or this DPA when Processing CompanyCam Data.

2.3. **Details of Processing.** The subject matter of Processing of Personal Information by Service Provider is the performance of the: (1) Services pursuant to the Agreement; (2) Processing initiated by Data Subjects in their use of the

Services; and (3) Processing to comply with other documented instructions provided by CompanyCam (e.g., via email) where such instructions are consistent with the terms of the Agreement. The nature and purpose of the Processing will be included in each applicable statement of work or order form. The details of Processing are set forth in **Appendix 1** to this DPA.

2.4. **Service Provider's Use of CompanyCam Data.** Service Provider shall only access and use CompanyCam Data to the minimum extent necessary to perform its obligations as a Service Provider under the Agreement. Service Provider shall not:

2.4.1. retain, use, or disclose CompanyCam Data for any purpose other than for the specific business purposes provided in the Agreement;

2.4.2. process CompanyCam Data for commercial purposes other than as required to perform its obligations under the Agreement;

2.4.3. combine the CompanyCam Data it receives from or on behalf of CompanyCam with information that it receives from, or on behalf of, another person or persons or that Service Provider collects from its own interactions with Data Subjects;

2.4.4. retain, use, or disclose CompanyCam Data outside of Service Provider's direct relationship with CompanyCam;

2.4.5. sell or share CompanyCam Data (as defined in applicable Data Protection Laws);

2.4.6. re-identify any de-identified CompanyCam Data; or

2.4.7. use any CompanyCam Data, including any Personal Information, in connection with the use of any artificial intelligence (AI) technology or other large machine learning models, use CompanyCam Data to train any data sets or algorithms or use CompanyCam Data as input into any AI technology or large machine learning model without CompanyCam's express prior written consent.

2.5. **Certification.** Service Provider certifies to CompanyCam that it understands the requirements and restrictions of this Section 2 and the restrictions set forth in Section 1798.140(ag) of the CCPA and shall comply with them.

3. Handling CompanyCam Data

3.1. **Ownership of CompanyCam Data.** As between the Parties and where permitted under applicable law, CompanyCam is and will remain the sole and exclusive owner of all CompanyCam Data which is Processed by Service Provider under this Agreement. Service Provider has no ownership rights in or to CompanyCam Data or any derivatives thereof.

3.2. **De-identified Information.** Service Provider and its Personnel may not create de-identified or aggregated information using CompanyCam Data without CompanyCam's prior written consent.

4. Data Subject Rights Requests

4.1. **Response to Data Subject Rights Requests.** Service Provider shall promptly (in no more than three calendar days) notify CompanyCam of any Rights Request that Service Provider receives regarding CompanyCam Data. Service Provider shall: (i) permit CompanyCam to have sole control over any response to a Rights Request, including the timing, method, and content; (ii) not respond directly to a Rights Request unless expressly requested by CompanyCam or where required to do so by applicable law; and (iii) comply with any request made by Controller relating to Personal Information in

connection with a Rights Request (e.g., Service Provider shall delete or correct Personal Data of Data Subjects if and when requested by CompanyCam).

4.2. **Assistance.** Service Provider shall assist CompanyCam in responding to Rights Requests in accordance with the Data Protection Laws and this DPA.

5. Service Provider Personnel

5.1. **Confidentiality.** Service Provider requires its Personnel to treat CompanyCam Data as Confidential Information. Service Provider shall ensure that its Personnel engaged in the Processing of CompanyCam Data are informed of the confidential nature of the CompanyCam Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Service Provider shall (i) ensure that such confidentiality obligations are consistent with the obligations under the Agreement and this DPA and that those obligations extend beyond the time period that such Personnel perform Services for Service Provider; (ii) use commercially reasonable efforts to ensure the reliability of any Personnel engaged in the Processing of CompanyCam Data; and (iii) provide training regarding the Data Protection Laws to Personnel Processing CompanyCam Data under the Agreement on at least an annual basis. Service Provider is responsible for its Personnel and will be liable to CompanyCam if its Personnel violate the terms of the Agreement, this DPA, Data Protection Laws or cause damages resulting from a Security Incident.

5.2. **Limitation of Access.** Service Provider shall ensure that access to CompanyCam Data is limited to those Personnel responsible for providing the Services under the Agreement.

6. Data Security Protections

6.1. **Security Measures.** Service Provider will develop and maintain a Security Program. The Security Program must, at a minimum include the requirements set forth in **Appendix 2** and include: (i) limits on access to CompanyCam Data; (ii) security for all systems, including without limitation, business facilities, data centers, paper files, servers, back-up systems and computing equipment, including all mobile devices and other equipment with information storage capability; (iii) implementing network, device, application, database and platform security; (iv) securing information transmission, storage and disposal; (v) implementing authentication and access controls within media, applications, operating systems and equipment; (vi) pseudonymization and encryption of CompanyCam Data at rest and in transit; (vii) pseudonymization and encryption of CompanyCam Data transmitted over public or wireless networks; (viii) conducting penetration testing and vulnerability scans to then-current NIST standards and promptly implementing, at Service Provider 's sole cost and expense, a corrective action plan to correct the issues that are reported as a result of the testing; (ix) implementing appropriate Personnel security and integrity procedures and practices, including conducting background checks consistent with applicable law; (x) ensuring the ability to restore the availability and access to CompanyCam Data in a timely manner in the event of a physical or technical incident, including a Security Incident; and (xi) establishing a process for regularly auditing, testing, assessing and evaluating the Security Program and the effectiveness of the technical and organizational measures for ensuring the security of the Processing.

6.2. **Ongoing Compliance Monitoring.** Service Provider will regularly monitor compliance with its Security Program. Service Provider will not materially decrease the overall scope of its Security Program during the term of the Agreement. Service Provider must keep its Security Program current in light of changes in relevant technology and the Data Protection Laws. Service Provider shall provide CompanyCam evidence of such activities upon request.

6.3. **Other Policies**. Service Provider and its Personnel shall comply with any additional CompanyCam policies, standards and procedures communicated by CompanyCam to Service Provider related to the Services under this Agreement, such as acceptable use policies, information security policies, and password policies. CompanyCam reserves the right to revise such policies at any time.

7. Sub-Processors

7.1. **Use of Sub-Processors.** Service Provider may not engage any Sub-Processors to Process CompanyCam Data under this Agreement without the prior written consent of CompanyCam. In the event CompanyCam consents to the use of a Sub-Processor, Service Provider shall enter into a written agreement with each Sub-Processor containing data protection obligations at least as protective as those in the Agreement and this DPA. Upon CompanyCam's written request, Service Provider will provide CompanyCam with copies of such agreements. Service Provider must list all Sub-Processors with access to CompanyCam Data in **Appendix 3** to this DPA and include any Sub-Processor's name, location, and contact information for the person responsible for privacy and data protection compliance at that Sub-Processor.

7.2. **New Sub-Processors.** In the event that Service Provider proposes to engage additional Sub-Processors to assist in the Processing of CompanyCam Data during the Term, Service Provider will notify CompanyCam in writing. CompanyCam will have thirty (30) days from the date of such notification to object to the engagement of any new Sub-Processor. If CompanyCam consents in writing, that Sub-Processor will be deemed added to **Appendix 3**. If CompanyCam objects, the Parties shall work in good faith to resolve CompanyCam's concerns. If the Parties cannot reach a good faith resolution, CompanyCam may require Service Provider to identify an alternative Sub-Processor which is acceptable to CompanyCam, or CompanyCam may terminate this Agreement with no further obligation to Service Provider.

7.3. **Liability.** Service Provider shall be responsible for any breach of the obligations set forth in this DPA and any violation of Data Protection Laws by a Sub-Processor to the same extent as if Service Provider had caused such breach or violation.

8. International Data Transfers and Restricted Transfers.

8.1. **Incorporation of Standard Contractual Clauses.** If CompanyCam transfers of the Personal Data of residents of the European Economic Area ("EEA" includes all EU member states, plus Iceland, Liechtenstein, and Norway), the United Kingdom or Switzerland to a country that is outside of the EEA, the United Kingdom, or Switzerland (as applicable), the transfer shall take place pursuant to Module 2 of the Standard Contractual Clauses (Controller to Processor) or Module Three of the Standard Contractual Clauses (Processor to Processor), which are incorporated by reference in a format which is mutually agreeable to the Parties and in compliance with applicable Data Protection Laws, unless such transfer is to a country that ensures an adequate level of data protection and such country is in receipt of a valid adequacy decision from the European Commission, the United Kingdom, and/or the Swiss Supervisory Authority as applicable. CompanyCam authorizes only the transfers set out in **Appendix 1** to this DPA.

In addition, the Parties agree that the following optional clauses are incorporated into the EU Standard Contractual Clauses:

a. Clause 7 (where module 3 is applicable): docking clause, shall apply.
b. Clause 9 option (2): specific prior authorization for Sub-Processors and the Parties agree that the timeframe for requesting the specific authorization shall be 30 days;

c. Clause 17 (Governing law): the clauses shall be governed by the laws of Ireland;

d. Clause 18 (Choice of forum and jurisdiction): the courts of Ireland shall have jurisdiction.

8.2. **Transfers of UK Personal Data.** In respect of transfers of UK Personal Data, the Parties agree to comply with the obligations set out in the EU Standard Contractual Clauses as amended by the UK Addendum, which is incorporated by reference, as though they were set out in full in this Agreement, with CompanyCam as the "exporter" and Service Provider as the "importer."

8.3. **Alternative Transfer Mechanisms.** In the event that the Parties engage in transfer of EU Personal Data, Swiss Personal Data, or UK Personal Data outside the Protected Area and a relevant European Commission decision or other valid adequacy method under applicable Data Protection Laws on which CompanyCam has relied in authorizing the data transfer is held to be invalid, or that any Supervisory Authority requires transfers of Personal Data made pursuant to such decision to be suspended, then CompanyCam may, at its discretion, require Service Provider to cease Processing Personal Data to which this paragraph applies, or cooperate with it and facilitate use of an alternative transfer mechanism.

9. Response to Complaints and Requests from Supervisory Authorities

9.1. **Complaints.** In the event that Service Provider receives any official complaint, notice, or communication that relates to Processing of CompanyCam Data, (including from a Data Subject or Supervisory Authority) in connection with the Agreement, to the extent legally permitted, Service Provider shall promptly notify CompanyCam. Service Provider shall provide CompanyCam with reasonable cooperation and assistance in relation to any such complaint, notice, or communication.

9.2. **Notice of Inquiries.** Service Provider shall inform CompanyCam without undue delay of requests, audits, subpoenas, or other inquiries from a Supervisory Authority in relation to CompanyCam Data or Processing of CompanyCam Data.

9.3. **Cooperation with Supervisory Authorities.** Service Provider and its Personnel shall cooperate with any audit, review, investigation, or other activity undertaken by a Supervisory Authority pertaining to the Processing of CompanyCam Data under this DPA.

10. Cooperation and Audit Rights

10.1. **Cooperation/Questionnaire.** Service Provider shall promptly and completely respond to CompanyCam's requests for information about Service Provider's data security practices, privacy practices, and any automated decision- making technology used in providing the Services. This includes responding to requests relevant to completing any legally required cybersecurity audit or risk assessment related to its Security Program or its Processing of CompanyCam Data under this Agreement. In addition, upon the request of CompanyCam, Service Provider shall complete a data security questionnaire or similar assessment at least once per calendar year. Upon CompanyCam's request, Service Provider will also provide relevant documents and make its Personnel, including Sub-Processors, available to discuss its responses to such questionnaires or assessments.

10.2. **Data Security Audit Standards**. Service Provider shall submit to an independent, reputable third-party audit governed by the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 18 (SOC 1 Type II and SOC 2 Type II) and the

International Standard on Assurance Engagements 3402 (ISAE 3402) (in accordance with the requirements of the International Federation of Accountants (IFAC)) (or mutually agreed upon equivalents) and obtain certificates of compliance on an annual basis. Service Provider shall provide CompanyCam with a copy of the most recent available audit report conducted pursuant to this Section 10.2 at least annually and any time upon request. If the audit identifies any critical or high-risk vulnerabilities, Service Provider shall provide notice to CompanyCam and shall work continuously to remediate those issues, provided that CompanyCam shall have the right to terminate the Agreement upon written notice as a result of such vulnerabilities. Service Provider shall also provide CompanyCam with the results of any penetration testing performed by Service Provider upon CompanyCam's request. CompanyCam will treat Service Provider 's audit reports and penetration testing results as Confidential Information under the Agreement.

10.3. **CompanyCam's Audit Rights.** At least once per calendar year, or at any time after a Data Security Incident, Service Provider shall permit CompanyCam to monitor Service Provider's compliance with the requirements under this DPA and the Data Protection Laws. Such monitoring may include, without limitation, ongoing manual reviews, automated scans, and regular assessments, audit rights, receipt of results of penetration testing, or other technical and operational testing. Should CompanyCam become aware of any unauthorized use of Personal Information, CompanyCam has the right, upon reasonable notice to Service Provider, to stop and remediate Service Provider's (or its Sub-Processor's) such unauthorized use.

10.4. **Data Protection Impact Assessment.** At CompanyCam's request, Service Provider shall provide reasonable assistance and cooperation to CompanyCam in completing any data protection impact assessments, transfer impact assessments, or similar assessments as required by applicable Data Protection Laws.

11. Data Security Incident

11.1. **Security Incident.** In the event that Service Provider becomes aware of a Security Incident which impacts CompanyCam Data or CompanyCam's IT Infrastructure, Service Provider shall take the following actions:

11.1.1. Promptly, and in no more than 48-hours, communicate the nature of the Security Incident to CompanyCam, including a description of the Security Incident;

11.1.2. In the event that applicable Data Protection Laws require CompanyCam to notify individuals impacted by a Security Incident, or Supervisory Authorities of a Security Incident, or if requested by CompanyCam, Service Provider will assist CompanyCam with mitigating damages resulting from a Security Incident;

11.1.3. Between the Parties, CompanyCam shall have sole control over the timing, content, and method of providing notification to the impacted individuals and governmental authorities of a Security Incident; and

11.1.4. For any Security Incident resulting from the acts or omissions of Service Provider or its Personnel, (including its Sub-Processors), in addition to any other remedies available to CompanyCam at law or in equity, Service Provider shall: (a) take any corrective actions necessary to remedy the Security Incident; and (b) reimburse CompanyCam for its outofpocket costs and expenses arising from or related to the Security Incident, including but not limited to: (1) CompanyCam's costs incurred in notifying impacted individuals, Supervisory Authorities and credit bureaus; (2) CompanyCam's attorneys' fees and public relations fees incurred in responding to a Security Incident; (3) CompanyCam's costs of obtaining credit monitoring services and identity theft insurance for the benefit of the impacted individuals; (4) call center support required by law to

notify impacted individuals for ninety (90) days; (5) all fines, penalties or charges assessed by a Supervisory Authority; and (6) forensic IT and e-discovery services used by CompanyCam relating to the Security Incident. All of the foregoing will be considered direct damages for purposes of the Agreement.

12. Return or Deletion of CompanyCam Data

12.1. **Deletion of CompanyCam Data.** At the termination or expiration of the Agreement, Service Provider shall permanently delete all CompanyCam Data in its possession or control, including all copies thereof, in compliance with then-current U.S. National Institute of Standards and Technology (**"NIST**") guidelines for media sanitization. Such deletion must occur no later than sixty (60) days from the termination or expiration of the Agreement, or if applicable, from the delivery of such CompanyCam Data to CompanyCam at the termination or expiration of the Agreement. Promptly after such deletion of CompanyCam Data, a c-suite employee of Service Provider shall certify compliance with this section in writing to CompanyCam.

12.2. **Return of CompanyCam Data.** At any time upon the request of CompanyCam, or if applicable, prior to deletion of CompanyCam Data in accordance with Section 12.1, Service Provider shall promptly provide all CompanyCam Data in Service Provider 's and its Personnel's possession or control to CompanyCam at no additional charge, in any format requested by CompanyCam so long as such format is a standard and secure format.

13. Changes in Data Protection Laws

13.1. The Parties acknowledge that the Data Protection Laws as of the DPA Effective Date may change during the term of the Agreement. The Parties shall comply with any and all such changes to the extent applicable to the Processing of CompanyCam Data under the Agreement and this DPA, including, without limitation, entering into any necessary amendments to this DPA and/or separate agreements to the extent necessary to comply with such changes.

14. IT Infrastructure Security

14.1. **IT Infrastructure Access**. CompanyCam owns and operates an IT Infrastructure. The data stored in the IT Infrastructure includes CompanyCam Data Processed under the Agreement and this DPA. In order to maintain the security and integrity of its IT Infrastructure, CompanyCam strictly limits third-party access to its IT Infrastructure to only those service providers which have an absolute need to access the IT Infrastructure to perform services for CompanyCam. CompanyCam may deny, change, revoke or terminate Service Provider's, its Personnel's or its Sub-Processor's access to the IT Infrastructure, at any time, at the sole discretion of CompanyCam, without cause or advance notice. Service Provider shall only access and use the portions of the IT Infrastructure to the extent necessary to perform its obligations under the Agreement and this DPA and for no other purpose. Under no circumstances will Service Provider, its Personnel or its Sub-Processors attempt to access or use any portion of the IT Infrastructure, other than as expressly authorized in advance and in writing by CompanyCam.

14.2. **Protection of the IT Infrastructure.** Service Provider shall ensure that in performing the Services, neither Service Provider, its Personnel or its Sub-Processors, by any act or omission, adversely affect or alter the operation, functionality or technical environment of the IT Infrastructure. Service Provider, its Personnel and its Sub-Processors will not use the IT Infrastructure in any way that will subject CompanyCam to any criminal or civil liability. Service Provider agrees to comply with and cause its Personnel and Sub-Processors to comply with, all CompanyCam policies that are applicable to the use of and access to CompanyCam's IT Infrastructure.

14.3. **Risk of Loss.** In accessing and using the IT Infrastructure, Service Provider shall

be responsible to CompanyCam for any of the following resulting from the acts or omissions of Service Provider, its Personnel or its Sub-Processors: (i) any loss or corruption of any data stored on, accessed with, or transmitted through the IT Infrastructure; (ii) any substantial disruption to the IT Infrastructure which materially impacts CompanyCam's business operations or CompanyCam Data; (iii) any damages to CompanyCam, its Affiliates, its customers, or Personnel; and (iv) any damages resulting from unauthorized third- party access to the IT Infrastructure, or the CompanyCam Data. If CompanyCam determines that Service Provider, its Personnel, or Sub-Processors has violated any provisions related to the security of the IT Infrastructure, Service Provider shall assist CompanyCam in identifying the abuse and rectifying the harm.

15. Miscellaneous

15.1. **DPA Term and Survival.** This DPA shall be in effect during the term of the Agreement. The provisions of this DPA which by their nature are intended to survive the expiration or earlier termination of this DPA shall continue as valid and enforceable obligations of the Parties.

15.2. **Controlling Terms.** In the event of conflict between this DPA and the Agreement, this DPA shall control.

Appendix 1

DETAILS OF PROCESSING

1. **List of the Parties**

   The Parties to this agreement are CompanyCam and Speedshop. Their signatures to and date of this Agreement shall be deemed to be their signature to and date of the Standard Contractual Clauses.

2. **The Nature and Purpose for Processing the Personal Information**:

   To provide Services to CompanyCam pursuant to Article 2 of the Agreement.

3. **Categories of Data Subjects whose Personal Information is Transferred**:

   CompanyCam web and mobile application users.

4. **Categories of Personal Information to be Transferred:**

   4. Contact Information, subscription records, contents of in-app messages, internet activity, analytic data, targeted advertising data, device information, photos taken in the application, professional or employment information about the application users.

5. **Sensitive Data to be Transferred (if applicable):**

   Precise geolocation data.

6. **Duration of the Processing:**

   Term of the Agreement

7. **Frequency of the transfer**

   Continuous

8. **Nature of the processing/processing operations**

   Provision of the Services as described in Article 2 of the Agreement.

9. **Purpose of the data transfer and further processing**

   To provide the Services as described in the Agreement

10. **Retention period for Personal Data transferred, or criteria used to determine that period**

    Term of the Agreement

11. **EU Standard Contractual Clauses only: Competent supervisory authority**

    For EU Personal Data: the Supervisory Authority of Ireland;
    For Swiss Personal Data: the Swiss Federal Data Protection and Information Commissioner.
    For UK Personal Data: United Kingdom

Appendix 2

Technical and Organizational Measures

[Service Provider to provide description of technical and organizational measures]

Protecting Information

This policy outlines how The Speedshop protects company and client data.

Who does this apply to?

Everyone at The Speedshop - employees and contractors.

What we do:

1. **Encrypt everything**
    - Use full disk encryption on all devices. For Mac, use FileVault.
2. **Control access**
    - Use strong, unique passwords.
    - Enable multi-factor authentication (MFA) when available
    - Use a password manager.
3. **Handle data carefully**
    - Back up critical data regularly
    - Delete client data when the contract ends.
    - Only store client data in our “blessed” systems - e.g. the client_notes repository, not in random/ad-hoc locations.
4. **Stay sharp**
    - Complete yearly security training.
    - Report security incidents immediately to Nate.

Keep it current

We'll review this policy every year and update as needed.

Training

As a small company, we keep security training simple and practical.

Annual review

Once a year, we:

1. Read through our security policy
2. Discuss any changes or new threats
3. Update our practices as needed

Ongoing learning

Throughout the year:

- Share relevant articles or news about security
- Discuss security implications of new projects

External resources

Once a year, we'll review:

- OWASP Top 10 for web app security
- National Cyber Security Centre (NCSC) small business guide
- Cybersecurity & Infrastructure Security Agency (CISA) resources

Incident simulation

Once a year, run a simple "what-if" scenario:

- "What if we lost a company laptop?"
- "What if a client's data was compromised?"

Documentation

Keep a simple log of all training activities. Note date, topic, and any decisions made.

Security is an ongoing conversation, not just an annual chore.

Asset Management

This policy outlines how we track, use, and protect our company assets.

What's an asset?

Anything valuable to our business:

- Hardware (laptops, phones, servers)
- Software and licenses
- Data (ours and clients')
- Intellectual property

How we manage assets

1. Keep an inventory
    - We manage client IP and data through the client_notes repository
    - Software: our company password manager list acts as an inventory
    - Hardware: See the Company Hardware Asset spreadsheet
    - Update when we get or dispose of anything
2. Control software
    - Discuss security implications when adding to this.
    - All software must have a password manager entry.
3. Set clear ownership
    - All assets are assumed to be owned by Nate unless otherwise noted
    - Owner ensures proper use and protection
4. Review regularly
    - Check inventory every 6 months
    - Like other policies, we update this policy yearly or when big changes happen

If it's valuable to us or our clients, we track it and protect it.

Access Control

This policy outlines how we manage access to our systems and data.

Core principles

1. Least privilege
    - Give access only to what's needed for the job
    - Review access rights regularly
2. Strong authentication
    - Use multi-factor authentication (MFA) wherever possible
    - Require strong, unique passwords or passphrases
    - Always use a password manager
3. Regular audits
    - Check who has access to what every 6 months
    - Remove unnecessary access immediately

Practical steps

1. Passwords
    - Use a password manager
    - Generate random, unique passwords for each account
    - Minimum 14 characters, mix of types
    - Passphrases are OK
2. Accounts
    - Create individual accounts for each person
    - No shared accounts unless required by client, even for testing
3. Admin access
    - Limit admin rights to absolute minimum
    - Use admin accounts only when necessary
4. Client data
    - For now, since all employees work on all clients, there is no fine-grained access control here.
5. Third-party services
    - Approve services before use
    - Use SSO when available
6. Offboarding
    - When someone leaves:
        i. Ensure they have all source deleted from laptop
        ii. Go through each password manager entry and remove the account
        iii. For each hardware asset, ensure access is removed
    - Change shared passwords, if (hopefully not) any.

Incident Response Plan

This plan outlines how we handle security incidents.

What's an incident?

Anything that threatens our data or systems:

- Malware or virus detection
- Unauthorized access attempts
- Data loss or theft
- Phishing attacks
- Unexpected system behavior

Response steps

1. Detect and report
    - Stay alert for unusual activity
    - Report concerns immediately, no matter how small
2. Assess and categorize
    - Determine the incident's severity and scope
    - Decide if it needs immediate action
3. Contain the threat
    - Change compromised passwords
4. Investigate
    - Gather information about the incident
    - Document everything you find
5. Resolve and recover
    - Remove threats (malware, unauthorized access)
    - Restore from backups if needed
    - Patch vulnerabilities
6. Disclosure
    - Disclose incident to affected clients, if any
7. Learn and improve
    - Review what happened and why
    - Update our practices to prevent similar incidents

Communication

- Internal: Keep the team informed
- External: Notify clients if their data is affected
- Legal: Consult if required by regulations

Key contacts

- Nate Berkopec / 090-8416-1631
- Legal Counsel: あしたの獅子法律事務所　ASHITA NO SHISHI LEGAL OFFICE 06(7777)1642 tsujino@ashitanoshishi.com

Act fast, but think clearly. Document everything.

Cryptography

These guidelines outline our approach to using cryptography to protect data.

When to use encryption

1. Data at rest
    - Full disk encryption on all devices, including phones and computers.
    - Encrypted backups. Ensure the above backups are encrypted.
    - Encrypted cloud storage, where available
2. Data in transit
    - We don’t have an encrypted chat channel yet, we will be evaluating vendors here
3. Sensitive data
    - Client source code (already happening if you’re full disk encrypting)
    - Financial information
    - Personal data

Key management

1. Generate strong keys
    - Use built-in OS tools or reputable key management software
    - Avoid manual key creation
2. Store keys securely
    - Use a password manager for personal keys
    - Consider a dedicated key management system for business keys
3. Rotate keys regularly
    - Change encryption keys at least annually
    - Rotate immediately if compromise is suspected
4. Use hardware keys
    - Yubikey NFC

When developing software

1. Use vetted cryptographic libraries
2. Don't invent your own crypto algorithms

Strong locks need strong keys. Protect your keys as you'd protect the data itself.

Physical and Environmental

This guide outlines how we protect our assets and data in a remote work environment.

Home office security

1. Workspace
    - Set up a dedicated work area
    - Keep it clean and organized
    - Set your devices to auto-lock within 5 minutes.
2. Network security
    - Use a strong Wi-Fi password
    - Enable WPA3 encryption if available
3. Physical security
    - Don’t leave your equipment unattended at cafes, coffee shops, etc

Equipment protection

1. Laptops and mobile devices
    - Use strong passcodes
    - Enable remote tracking and wiping, under your personal control (e.g. Find My for Mac)
    - Keep OS and software updated
2. Peripherals and storage
    - Encrypt external hard drives
    - Shred sensitive printed documents

Data handling

1. Digital files
    - Use company-approved cloud storage, do not use personal storage
2. Physical documents
    - Minimize printing of sensitive info
    - Use a cross-cut shredder for disposal
3. Artificial Intelligence
    - Exclude files from context which may potentially contain secrets.
    - Never send secrets or sensitive information to non-local AI models.

Travel and client visits

1. En route security

    - Use a privacy screen on planes/trains
    - Never leave devices unattended
    - Use a VPN, we can provision ProtonVPN for you
2. At client locations
    - Follow all client security protocols
    - Don't connect to client networks without approval
    - Be mindful of visual and audio privacy
3. Hotel stays
    - Use the room safe for devices when out
    - Use a VPN

Compliance

These guidelines help us meet legal requirements in the US, Japan, EU, and Australia.

Key regulations

1. EU: General Data Protection Regulation (GDPR)
2. US: New York SHIELD Act (for NY residents only)
3. Japan: Act on Protection of Personal Information (APPI)
4. Australia: Privacy Act 1988 and Australian Privacy Principles (APPs)

General compliance practices

1. Data minimization: Collect only necessary data
2. Purpose limitation: Use data only for specified purposes
3. Storage limitation: Delete data when no longer needed
4. Security measures: Implement appropriate technical and organizational measures
5. Do not store or handle personal information of clients or clients of our clients, anywhere.

Region-specific considerations

1. EU (GDPR)
    - We are an “occassional processor” under the law, so we do not have a GDPR representative.
    - We must maintain records of processing activities. In general, we should not be doing processing activities, consult Nate if you think we are doing this. All of our clients are told we have zero-day retention.
2. US
    - Generally only NY residents affected
    - We are not affected by the California law
3. Japan (APPI)
    - Nate is our Personal Information Protection Officer
    - If we have a breach, consult our legal counsel (Tsujino-san)
4. Australia (Privacy Act and APPs)
    - We are under the revenue threshold

Data access and deletion request policy

1. Receiving requests
    - Nate is point-of-contact
    - Accept requests via email at data@speedshop.co

    - Verify the identity of the requester
2. Processing access/deletion requests
    - Acknowledge receipt within 3 business days
    - Provide requested data within 30 days
    - Format: Provide data in a commonly used electronic format (depends on request)
    - Scope: Include all personal data held about the individual
        i. Generally: Mailchimp. See password manager for other possible storage locations.
    - Notify third parties: If data was shared, request they also delete the data
3. Exceptions
    - We deny requests if they are manifestly unfounded, excessive, or repetitive
    - We'll explain any denial in writing
4. Record keeping
    - Log requests and our responses in Drive
5. No fee
    - We process requests free of charge

Promptly forward any data requests you receive to Nate.

New Hire Checklist

1. Set up full disk encryption on all devices (e.g., FileVault for Mac)
2. Enable multi-factor authentication (MFA) on all accounts where available
3. Install and set up any password manager
4. If your job includes client travel, install and configure a VPN (ProtonVPN will be provisioned for you) and acquire a privacy screen for use on planes/trains
5. Enable remote tracking and wiping on laptops and mobile devices (e.g., Find My for Mac. Speedshop doesn't need to control the password/access, but you do.)
6. Set devices to auto-lock within at least 5 minutes
7. Enable WPA3 encryption on home Wi-Fi (if available)
8. Encrypt all external hard drives you use for work
9. If you will print anything, obtain a cross-cut shredder for sensitive document disposal
10. Get a Yubikey NFC for hardware key authentication (we will buy for you if required)
11. Set up company-approved cloud storage for work files (avoid personal cloud storage, use our Drive where possible)
12. Obtain contact information for Nate Berkopec, put it in your phone.
13. Update your OS on all devices
14. Ensure your home Wi-Fi has a strong password

APPENDIX 3

SUB-PROCESSORS

Instructions: Service Provider to list each Sub-Processor, including the name, address, phone number and email address for the person responsible for data protection issues related to the processing of CompanyCam Data at each such Sub-Processor.

No sub-processors