Data Processing Addendum
to the Neatoware General Terms and Conditions
Version 2026-08-16

This Data Processing Addendum ("DPA") forms part of the Neatoware General Terms and Conditions ("Conditions") and each Product and Services Agreement, Plan, Order, Schedule, Statement of Work, or other arrangement that incorporates or is subject to it (collectively, the "Agreement") between Neatoware LLC ("Neatoware," "Consultant," "We," "Us," or "Our") and the Client ("Client," "Customer," "You," or "Your").

1. PURPOSE AND SCOPE

This DPA automatically applies to the extent Neatoware Processes Personal Data on behalf of Client in connection with the Services. The CJIS provisions in Section 12 automatically apply whenever the Services involve direct or indirect access to, Processing of, storage of, transmission of, or administration of systems containing Criminal Justice Information (CJI).

This DPA allocates responsibilities concerning Personal Data and CJI. It does not expand the scope of the Services or require Neatoware to provide a service, control, platform, assessment, or certification that is not included in the Agreement or required by applicable law or an executed Required CJIS Document.

This DPA is intended to address generally applicable United States and Georgia data-protection requirements and applicable CJIS and GCIC requirements. It is not, by itself, intended to constitute a HIPAA business associate agreement, GDPR Article 28 processor agreement, CCPA/CPRA service-provider or contractor addendum, or any other jurisdiction-specific or industry-specific agreement. If such requirements apply, the parties will execute appropriate supplemental terms.

2. DEFINITIONS

Capitalized terms not defined in this DPA have the meanings assigned in the Conditions or the Agreement.

“Applicable Data Protection Law” means the federal and state privacy, data-security, breach-notification, records-protection, and criminal-justice-information laws, regulations, rules, and binding governmental requirements applicable to Neatoware’s Processing of Personal Data or CJI under the Services.

"Criminal Justice Information" or "CJI" means information defined as CJI under the FBI CJIS Security Policy, applicable Georgia law, and applicable Georgia Crime Information Center requirements, including criminal history record information and other information related to the administration of criminal justice.

"Personal Data" means information relating to an identified or identifiable natural person that Neatoware Processes on behalf of Client in connection with the Services.

"Processing" or "Process" means accessing, collecting, viewing, recording, organizing, storing, hosting, using, modifying, retrieving, transmitting, disclosing, backing up, restoring, returning, deleting, or otherwise handling Personal Data or CJI.

"Required CJIS Documents" means the official FBI CJIS Security Addendum, any CJA/G-NCJA and Vendor CJIS Network & Data Agreement, required contractor-employee certifications or acknowledgments, and any other agency-specific agreement, form, or written requirement that must be executed or accepted for the applicable CJI engagement.

"Security Incident" means a Security Incident as defined in the Conditions that affects Personal Data, CJI, or a system used to Process Personal Data or CJI.

"Subprocessor" means a third party engaged by Neatoware to Process Personal Data or CJI on behalf of Client in connection with the Services.

"Unsuccessful Security Event" has the meaning assigned in the Conditions.

3. PROCESSING INSTRUCTIONS AND PURPOSES

Neatoware will Process Personal Data and CJI only as reasonably necessary to:

- Provide and administer the contracted Managed Services, RMM, monitoring, support, backup, recovery, remote access, security, hosting, communications, consulting, and related Services;
- Maintain, secure, support, troubleshoot, document, and recover systems that Process such information;
- Detect, investigate, contain, and respond to security threats and operational failures within the contracted scope;
- Comply with Client's documented instructions, Applicable Data Protection Law, and applicable CJIS requirements; and

- Perform and administer the Agreement and this DPA.

The Agreement, its Schedules, approved Service Requests, written instructions from an authorized Client representative, Client-approved configurations, and binding instructions from an authorized governmental authority constitute documented instructions for purposes of this DPA.

Neatoware will not Process Personal Data or CJI for an unrelated purpose without Client's prior written instruction, except as required by law or an applicable CJIS requirement.

4. CLIENT RESPONSIBILITIES

Client is responsible for:

- Ensuring that it has lawful authority to collect, use, disclose, and Process Personal Data and CJI and to engage Neatoware to Process such information;
- Providing required notices and obtaining required consents, authorizations, approvals, and governmental permissions;
- The accuracy, quality, legality, classification, and permitted use of information made available to Neatoware;
- Identifying material categories of sensitive or regulated information and communicating special handling, access, retention, legal-hold, or agency restrictions;
- Determining appropriate business, legal, access, retention, recovery, notification, and risk-acceptance requirements; and
- Providing timely access, information, credentials, instructions, approvals, and cooperation reasonably required for Neatoware to perform the Services.

Client retains final authority over material business, legal, regulatory, notification, restoration, shutdown, and risk-acceptance decisions, subject to Neatoware's emergency-containment authority under Section 5.

5. SECURITY MEASURES

Neatoware will implement and maintain reasonable administrative, technical, and physical safeguards designed to protect Personal Data and CJI against unauthorized

access, acquisition, use, disclosure, alteration, loss, destruction, or material disruption. Safeguards will be appropriate to the nature of the Services, the information involved, the risks presented by the Processing, and applicable legal and CJIS requirements.

Neatoware will use least-privilege access, multi-factor authentication, logging, credential protection, monitoring, endpoint or network safeguards, backup controls, and other measures to the extent included in the contracted Services, reasonably available, technically supported, or required by applicable law or CJIS requirements.

Client remains responsible for its overall security posture and for systems, users, vendors, facilities, data, and controls outside Neatoware's contracted scope. Where the applicable Agreement includes a Shared Responsibility Matrix, the parties' operational roles are further described in that Matrix.

Client retains final authority over material business, legal, regulatory, notification, restoration, shutdown, and risk-acceptance decisions. Notwithstanding the foregoing, Neatoware may take immediate and proportionate technical containment measures when reasonably necessary to prevent imminent harm, limit an actual or reasonably suspected Security Incident, preserve evidence, maintain the security or integrity of the Services, or comply with applicable law or binding CJIS, GCIC, or governmental requirements. Neatoware will notify Client of any such action as soon as reasonably practicable.

6. SUBPROCESSORS

Client generally authorizes Neatoware to engage Subprocessors reasonably necessary to provide the Services. Neatoware will require each Subprocessor to be bound by written confidentiality, security, use, retention, deletion, and incident-notification obligations appropriate to the services performed and materially consistent with Neatoware's applicable obligations under this DPA.

Neatoware will maintain a current list of Subprocessors and provide it to Client upon request. Neatoware will provide reasonable advance notice of a material change involving a Subprocessor that will routinely host or have logical access to Personal Data or CJI, unless an urgent security, continuity, legal, or vendor condition makes advance notice impracticable. Client may raise reasonable, documented security or legal concerns, and the parties will work in good faith to address them.

Neatoware remains responsible for the performance of its Subprocessors to the extent required by Applicable Data Protection Law and the Agreement. A Subprocessor may

access CJI only as permitted by the Required CJIS Documents and applicable CJIS requirements.

Notices concerning new or replacement Subprocessors are Operational Notices under the Conditions and may be delivered to Client's Notice Email.

7. ASSISTANCE AND INDIVIDUAL RIGHTS

Taking into account the nature of the Processing and the Services, Neatoware will provide reasonable assistance to Client in responding to legally valid requests concerning Personal Data and in meeting applicable security, investigation, assessment, notification, or reporting obligations. Unless required otherwise by law or the Agreement, assistance beyond the ordinary scope of the Services is billable at Neatoware's applicable Rates.

8. SECURITY-INCIDENT NOTIFICATION

Neatoware will notify Client without unreasonable delay after discovering a Security Incident and, where required by applicable Georgia law, no later than twenty-four (24) hours after discovery.

Neatoware may provide information in phases as its investigation proceeds. To the extent reasonably available, notice will describe the nature of the Security Incident, the information and systems known to be affected, the known or approximate date of occurrence and discovery, the containment or response measures taken, and a contact for follow-up. Neatoware will provide reasonable updates as material information becomes available.

Neatoware is not required to notify Client of an Unsuccessful Security Event unless notification is required by law, an applicable CJIS requirement, or another binding provision of the Agreement, or unless the event materially disrupts the Services or forms part of a pattern reasonably indicating a Security Incident.

Notification under this Section does not constitute an admission of fault or liability.

Method of Notification. A notice under this Section is an Operational Notice under the Conditions and may be delivered to Client's Notice Email, through a secure portal, ticketing or security-management system, by telephone followed by written electronic confirmation, or by another method reasonably calculated to reach Client. Such notice is not required to comply with the Formal Legal Notice procedures in the Conditions. For

purposes of an applicable notification deadline, notice is given when transmitted to Client's Notice Email or another agreed electronic system, provided that Neatoware does not receive a delivery-failure notification. For a material Security Incident or an incident requiring immediate Client action, Neatoware will also use reasonable efforts to contact an appropriate Client representative using another contact method reasonably available in Neatoware's records.

9. RETURN AND DELETION

Upon expiration or termination of the applicable Services, Neatoware will, at Client's written election and within a commercially reasonable period, either: (a) return a copy of the Personal Data and CJI to Client and delete Neatoware's remaining copies; or (b) delete the Personal Data and CJI without returning a copy. Return and deletion remain subject to the retention, backup, legal-preservation, and CJIS exceptions stated below.

Routine deletion in accordance with this Section will be performed without an additional charge. Extraordinary export, conversion, reconstruction, organization, restoration, media, transmission, migration, or transition assistance is billable at Neatoware's applicable Rates.

Client shall provide its election within thirty (30) days after termination. If Client does not provide a timely election, Neatoware may delete the information in accordance with this Section.

Neatoware may retain information only to the extent required by applicable law, court order, or a legally enforceable preservation obligation. Retained information will remain protected under this DPA, will not be used for an unrelated purpose, and will be deleted when the applicable retention obligation expires.

Information contained in routine backups that cannot reasonably be isolated for immediate deletion may remain until deleted through the ordinary backup-retention and overwrite cycle. Until deleted, the information remains subject to this DPA and will not be restored or accessed except for legitimate backup, recovery, security, legal, or continuity purposes.

Return and deletion of CJI are subject to the Required CJIS Documents and applicable CJIS requirements, which control if they require a different or faster disposition.

10. AUDIT AND INFORMATION RIGHTS

Upon reasonable written request, Neatoware will make available information reasonably necessary to demonstrate compliance with this DPA. Client may conduct one routine compliance review during any twelve-month period, using available documentation, questionnaires, certifications, reports, and remote interviews before requesting an on-site audit.

The once-per-twelve-month limitation does not apply when an additional review is reasonably required because of a Security Incident, a regulator or CJIS request, reasonable documented evidence of material noncompliance, or verification of agreed remediation.

Any on-site audit must be conducted on reasonable notice, during Business Hours unless otherwise required, and in a manner that minimizes disruption and protects the confidentiality and security of Neatoware and other clients. Client is responsible for its audit costs and Neatoware's reasonable support costs, except to the extent the audit is required by law or a CJIS authority or identifies material noncompliance by Neatoware.

Nothing in this Section limits audit, inspection, information, or final-audit rights granted to an authorized governmental or CJIS authority under applicable law or a Required CJIS Document.

11. LIABILITY AND RELATIONSHIP TO THE CONDITIONS

Except solely to the extent expressly provided in this DPA or prohibited by applicable law, the limitations of liability, exclusions of damages, Aggregate Liability Cap, claim limitations, indemnification obligations, insurance provisions, confidentiality obligations, defenses, and other protective provisions of the Conditions apply fully to this DPA and to all claims arising out of or relating to Personal Data, CJI, Processing, Security Incidents, privacy, security, confidentiality, return or deletion of information, or Neatoware's performance or alleged failure to perform obligations under this DPA.

For avoidance of doubt, claims arising from or relating to Personal Data, CJI, privacy, data protection, cybersecurity, Security Incidents, unauthorized access, loss or corruption of information, breach notification, confidentiality, or regulatory obligations do not create a separate liability cap, separate pool of damages, or additional monetary remedy. Such claims are included within, and share, the Aggregate Liability Cap applicable under the Conditions.

Multiple claims arising from the same or related Security Incident, unauthorized access, vulnerability, event, act, omission, Processing activity, or series of related circumstances will be treated as related claims and will not increase or multiply the Aggregate Liability Cap.

Nothing in this DPA creates a separate or additional monetary liability, remedy, warranty, indemnification obligation, insurance obligation, or measure of damages beyond those expressly stated in the Agreement and the Conditions.

Nothing in this Section limits any compliance, access, suspension, audit, reporting, return, deletion, investigation, or enforcement right granted to an authorized governmental or CJIS authority under applicable law or a Required CJIS Document. Such regulatory or governmental rights do not, by themselves, create or enlarge a monetary claim or remedy in favor of Client beyond that otherwise available under the Agreement or applicable law.

12. CJIS ENGAGEMENTS AND REQUIRED DOCUMENTS

Whenever the Services involve CJI, the parties will execute or acknowledge the Required CJIS Documents applicable to the engagement before Neatoware or its personnel receive access to CJI or to systems for which such execution is required.

The Required CJIS Documents, the FBI CJIS Security Policy, applicable Georgia Crime Information Center requirements, and binding instructions of the authorized criminal-justice agency or CJIS authority govern access to and handling of CJI. This DPA supplements those requirements but does not replace, modify, restate, or reduce them.

If this DPA or another provision of the Agreement conflicts with a Required CJIS Document or an applicable CJIS requirement, the Required CJIS Document or CJIS requirement controls with respect to CJI. The provisions of this DPA concerning Subprocessors, Security Incidents, return and deletion, audits, suspension, termination, and other CJI matters apply only to the extent consistent with those controlling requirements.

Nothing in this DPA limits the authority or rights of the FBI, GBI, or GCIC, the applicable CJIS Systems Agency or CJIS Systems Officer, the contracting government agency, or another authorized governmental entity.

13. GOVERNING LAW AND ORDER OF PRECEDENCE

This DPA is governed by the laws of the State of Georgia, except to the extent another law mandatorily applies.

For matters concerning CJI, Section 12 controls. For a direct conflict concerning a Personal Data obligation, this DPA controls over the Conditions and any lower-ranking document under the applicable Agreement, except to the extent a signed amendment or custom Schedule or Exhibit expressly attached to and made part of the Agreement specifically identifies and modifies this DPA. In all other respects, the order of precedence stated in the applicable Agreement applies.

END OF DATA PROCESSING ADDENDUM