Complete with CWCO-SUP-CORE and ACORD 125/126. Answer all questions; if not applicable, indicate N/A. Completion of this application does not bind coverage.

COMPANY NAME	PRIMARY WEBSITE	NATURE OF BUSINESS (INDUSTRY)

COMPANY ADDRESS	CITY	STATE / ZIP	ADDITIONAL WEBSITES

CURRENT GROSS ANNUAL REVENUE ($)	PROJECTED ANNUAL REVENUE — NEXT 12 MO. ($)	EFFECTIVE DATE REQUESTED

A COMPANY & DATA PROFILE

A1 Are there any subsidiaries the Named Insured wishes to cover under this policy? ☐ Yes ☐ No

IF YES, EXPLAIN

Estimated number of records containing unique personally identifiable information stored, processed or transmitted by the applicant, including records held by third-party providers

☐ 0 – 250,000 ☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000
☐ 1,000,001 – 2,500,000 ☐ 2,500,001 – 5,000,000 ☐ 5,000,001 – 10,000,000
☐ Over 10,000,000 (state below) ☐ ☐

IF OVER 10 MILLION — ESTIMATE	DOES APPLICANT DERIVE MORE THAN 50% OF REVENUE FROM TECHNOLOGY PRODUCTS/SERVICES?

A2 Does the applicant collect, capture, purchase, or otherwise obtain biometric data (fingerprints, iris/retina scans, voiceprints, health/exercise data, DNA)? ☐ Yes ☐ No

IF YES, EXPLAIN

A3 Does the applicant engage in any activity involving cryptocurrency, token, digital coin, or similar — mining, trading, exchanging, or storing? ☐ Yes ☐ No

IF YES, EXPLAIN

A4 Does the applicant provide data processing, aggregation, storage or hosting services to third parties (managed services provider, data aggregator)? ☐ Yes ☐ No

IF YES, EXPLAIN

A5 If the applicant accepts payment cards, is the applicant or its outsourced payment processor PCI-DSS compliant? ☐ Yes ☐ No

B EMAIL & PERIMETER SECURITY

B1 Do you have email filtering in place? ☐ Yes ☐ No

B2 Do you use an advanced email security solution (Secure Email Gateway) with URL and attachment sandboxing? ☐ Yes ☐ No

IF YES, EXPLAIN

B3 Are all internet access points secured by firewalls? ☐ Yes ☐ No

B4 Do you restrict employees' and external users' system privileges and access to personal information on a business-need-to-know basis? ☐ Yes ☐ No

C BACKUP & RECOVERY

C1 Do you have a backup solution? ☐ Yes ☐ No

Backup frequency:

☐ Continuous ☐ Daily ☐ Weekly ☐ Monthly

Backup solution includes (check all that apply):

☐ Cloud-based backups ☐ Backup servers not joined to Windows domain ☐ Unique credentials for backup servers/accoun
☐ Copies stored in 2+ geographic locations ☐ Backup servers segmented from network ☐ Immutable backups
☐ Offline / air-gapped copy maintained ☐ MFA required for backup access ☐ None of these

C2 Do you perform backups of business-critical data on at least a weekly basis? ☐ Yes ☐ No

C3 Do you have a Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) in place? ☐ Yes ☐ No

IF YES, EXPLAIN

If yes to C3, state in the explanation field whether the plan has been tested in the last 12 months.

D ACCESS CONTROL & AUTHENTICATION

Multi-Factor Authentication (MFA) is enforced for (check all that apply):

- ☐ All remote access to the network
- ☐ Internal privileged accounts (admin, service
- ☐ Email access via webmail and non-corporate d
- ☐ Access to all critical applications
- ☐ User access to systems with sensitive data
- ☐ None of these

Privileged accounts are secured by (check all that apply):

- ☐ Separate admin / non-admin accounts per user
- ☐ Unique, complex local admin credentials on a
- ☐ Password management vault for privileged acc
- ☐ Standard users lack local admin rights
- ☐ Privileged Access Management (PAM) solution
- ☐ None of these

Sensitive data is protected by (check all that apply):

- ☐ Role-based least-privilege access
- ☐ MFA required for sensitive-data system acces
- ☐ Network segmentation of sensitive-data serve
- ☐ Logging and monitoring
- ☐ Encryption at rest (file level)
- ☐ Encryption of data in transit

E ENDPOINT & NETWORK SECURITY

Endpoint security technology in place (check all that apply and list vendor below):

- ☐ Standard antivirus
- ☐ Next-generation antivirus (NGAV)
- ☐ Endpoint Detection & Response (EDR)
- ☐ Extended Detection & Response (XDR)
- ☐ Managed Detection & Response (MDR)
- ☐ None of these

ENDPOINT SECURITY PRODUCT / VENDOR	MANAGED SECURITY PROVIDER (IF MDR)

E1 Do you have an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) in place? ☐ Yes ☐ No

E2 Do you conduct penetration testing of your network at least annually? ☐ Yes ☐ No

IF YES, EXPLAIN

E3 Do you conduct employee security or phishing training, for all employees, at least annually? ☐ Yes ☐ No

F FUNDS TRANSFER & SOCIAL ENGINEERING CONTROLS

F1 Prior to executing an electronic payment or funds transfer, do you verify the request with the requestor via a separate means of communication before transferring funds or making payment changes? ☐ Yes ☐ No

IF YES, EXPLAIN

F2 Is out-of-band verification required for any change to vendor banking or payment instructions? ☐ Yes ☐ No

IF YES, EXPLAIN

F3 If the applicant uses multimedia material provided by others, does it always obtain the necessary rights, licenses, releases and consents prior to publishing? ☐ Yes ☐ No

IF YES, EXPLAIN

G INCIDENT HISTORY

Attach a detailed addendum for any 'Yes' answer below.

G1 In the past three years, has the applicant experienced any cyber security incident, data privacy incident, or multimedia liability claim? ☐ Yes ☐ No

IF YES, EXPLAIN

G2 Does the applicant, or any person or organization proposed for this insurance, have knowledge of any actual or alleged security breach, privacy breach, or event that may reasonably be expected to give rise to a claim or costs? ☐ Yes ☐ No

IF YES, EXPLAIN

G3 In the past three years, has the applicant or any service provider with network access sustained an unscheduled outage or interruption lasting longer than 6 hours? ☐ Yes ☐ No

IF YES, EXPLAIN

G4 During the past 36 months, did any cyber incident cost more than $10,000 to rectify, or result in a lawsuit or formal dispute? ☐ Yes ☐ No

IF YES, EXPLAIN

G5 Has cyber or technology E&O coverage ever been declined, cancelled, or non-renewed? ☐ Yes ☐ No

IF YES, EXPLAIN

H ADDITIONAL INFORMATION

ANYTHING ELSE AN UNDERWRITER SHOULD KNOW — SECURITY CERTIFICATIONS (SOC 2, ISO 27001), INCIDENT RESPONSE RETAINER, OR PLANNED CHANGES

I REPRESENTATIONS & SIGNATURE

The undersigned declares that the statements and answers given in this supplemental are true, complete and correct to the best of their knowledge, and that no material fact has been withheld or misstated. The applicant agrees that this supplemental, together with all ACORD applications and attachments, forms the basis of any submission to insurers and may be relied upon by them. Signing this supplemental does not bind coverage. The applicant acknowledges that limits of liability may be reduced, and may be completely exhausted, by claim expenses.

FRAUD NOTICE: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information, or conceals for the purpose of misleading information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties. (State-specific fraud warnings apply; see state amendatory notice.)

APPLICANT / AUTHORIZED SIGNATURE (TYPE FULL NAME)	TITLE	DATE

PRODUCER — CORY WASHINGTON & CO. LLC	PRODUCER SIGNATURE (TYPE FULL NAME)	DATE