

## Cybersecurity Agreement

This Cybersecurity Agreement ("**Agreement**") is made and entered into this [day] day of [month] [year] ("**Effective Date**"), by and between Ingram Micro Inc., a Delaware corporation ("**Ingram Micro**"), and [company name] ("**Supplier**" or "you"). Ingram Micro and Supplier are sometimes hereinafter referred to individually as a "**Party**" and collectively as the "**Parties**."

**1. Scope.** The terms of this Agreement specify the minimum information protection practices to be employed by the Supplier and any third parties in association with Supplier with respect to the practices, systems, policies and all other related aspects of information security and privacy, data handling and protection processes and structures related to the relationship between Supplier and Ingram Micro.

### **2. Definitions.**

**2.1. "Affiliate Companies"** means any companies controlling, being controlled by, or under common control with another company.

**2.2. "Breach"** means: (i) the unauthorized acquisition, access, use or disclosure of Ingram Micro Data or Information Systems; (ii) disclosure of Ingram Micro Data, occurring directly or indirectly from the violation of the terms of this Agreement by Supplier, including any of its employees, agents, or independent contractors or affiliates; or (iii) violation of any applicable data protection law.

**2.3. "Data Processing Agreement"** means a legally binding document to be executed between the Parties that regulates the particularities of data processing of Personal Data including the scope and purpose of the Personal Data as well as the relationship between the Parties.

**2.4. "Discovered" or "Discovery"** means when a Breach or other Security Incident is first known to Supplier or, by exercising reasonable diligence, should have been known to Supplier.

**2.5. "CISO" or "Chief Information Security Officer"** means the head of a Party's Information Security or Cybersecurity team.

**2.6. "POC" or "Point of Contact"** means a member of a Party's CISO's staff who will be the principal point of contact to the other Party. The POC will be granted the authority to execute the terms and conditions of this Agreement on behalf of the Party.

**2.7. "Guidelines"** means the most recent version of the National Institute of Science and Technology ("**NIST**") Cybersecurity Framework ("**CSF**") as they may be updated and revised from time to time or its replacement as designed or recommended by the United States government should the NIST CSF be discontinued and replaced by another standard.

**2.8. "Ingram Micro Data"** means any data provided by Ingram Micro or any of its subsidiaries, suppliers, customers, or partners to Supplier in relation to the Agreement and any data created by the Supplier, either directly or indirectly for Ingram Micro or its subsidiaries, under the Agreement. Ingram Micro data includes, without limitation, all strategic information, financial statements, information or projections, business plans, data, business records, customer lists, supplier agreements, partnership or joint venture agreements, sales and marketing plans, employee lists, policies and procedures, information relating to processes, techniques, technologies, software programs, source code, schematics, designs, or theory and any or all other confidential or proprietary information. Ingram Micro Data includes Sensitive Data.

**2.9. "Personal Data"** means information that, when used alone or with other relevant data, can identify an individual. Personal Data is sometimes referred to as Personal Information or Personally Identifiable Information.

**2.10. "Sensitive Data"** means: (i) Personal Data, including, but not limited to, employee and customer data, as generally defined within industry or as defined by any regulation or regulatory body without limitation to its jurisdiction; (ii) trade secrets; (iii) United States public sector data (iv) data governed by laws or regulations of any country; or (v) any card used for payment (credit, debit, prepaid, stored value, gift or chip) including, but not limited to, any card bearing the logo of one of the PCI Security Standards Council's payment brands.

**2.11. "Security Event"** means an action or a log entry with a negative consequence or potentially negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, unauthorized access to Sensitive Data or execution of malicious code that destroys data.

**2.12. "Security Incident"** means any of the following: (i) an imminent threat or a violation of security policies, acceptable use policies, standard security practices as set forth in this Agreement; (ii) one or more credible Security Events; or (iii) a Breach.

**2.13. "Third Party(ies)"** means Supplier's Affiliate Companies and Supplier's contractors, agents, vendors and third-party service providers (i.e., subcontractors) used to perform the services.

**2.14. "Information System(s)"** means a set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

**3. Confidentiality.** Ingram Micro may grant access to Ingram Micro Information Systems or disclose Ingram Micro Data to Supplier, either orally, visually or in writing, or other tangible form. The Supplier may not grant access to Ingram Micro Information Systems or disclose Ingram Micro Data, without Ingram Micro's express written consent, to any person except to its and its Affiliates Companies' directors, officers, employees, agents, subcontractors, or consultants to whom it is necessary for such purposes (collectively, Supplier's "**Agents**"). Supplier must notify each of its Agents who receive access to Ingram Micro Information Systems or who receive Ingram Micro Data that such Agents must hold such access and such Ingram Micro Data in confidence and may not disclose it to others or permit others to use it for their benefit or the detriment of Ingram Micro. Supplier must take reasonable measures to maintain the confidentiality of the Ingram Micro Data, but not less than the measures it uses for its confidential information of similar type. This Agreement does not grant Supplier any license to use Ingram Micro Data or assets except for the limited purpose set forth in this Agreement.

**4. Ownership and Use of Data.** In connection with the Agreement, Supplier has received, may receive, or may have access to Ingram Micro Data, including but not limited to Sensitive Data, which information may be subject to regulatory protections. Ingram Micro Data is and will remain, as between the Parties, the property of Ingram Micro. Supplier will not possess or assert any lien or other right against or to the Ingram Micro Data. Supplier agrees not to permit access, or allow access to, or use of, any Ingram Micro Data except in furtherance of its obligations under the Agreement. No Ingram Micro Data, or any part thereof, will be sold, assigned, leased, or otherwise disposed of to third parties by Supplier or commercially exploited by or on behalf of Supplier. Ingram Micro Data may not be used by Supplier for any purpose other than for providing services directly or indirectly to Ingram Micro. Supplier agrees to promptly correct any errors or inaccuracies in the Ingram Micro Data and restore any losses of any Ingram Micro Data resulting directly or indirectly from Supplier's performance under the Agreement. Upon Ingram Micro's request to Supplier, Ingram Micro Data (including notes on and copies thereof) will be promptly returned to Ingram Micro in a form requested by Ingram Micro or, if Ingram Micro so elects, will be destroyed by Supplier. Upon termination of any agreement between the Parties, Supplier must immediately and securely destroy all Ingram Micro Data, unless there is a regulation or law that requires Supplier to retain such information. If the Supplier is required to retain Ingram Micro Data, Supplier will continue to comply with the provisions of this Agreement until such time the Ingram Micro Data may be destroyed. Supplier must securely delete, destroy, or render irrecoverable Ingram Micro Data using the U.S. Department of Defense 5220.22-M Wiping Standard or a comparable standard. Supplier must destroy physical media containing Ingram Micro Data using a method agreed in writing between the Parties.

**5. Safeguarding Ingram Micro Data.** Supplier will establish and maintain safeguards against the disclosure, destruction, loss, copying, or alteration of Ingram Micro Data in the care, custody, or control of Supplier that are no less rigorous than those maintained by Supplier for its own information of a similar nature.

**6. Cybersecurity Program.** Supplier's cybersecurity program includes, but is not limited to, equivalent to, or exceeding the Guidelines and the requirements set forth in this Section ("**Cybersecurity Program**"). Supplier must maintain: (i) security Controls; (ii) security countermeasures; (iii) security processes; (iv) security compliance programs; and (v) security tools. Supplier's Cybersecurity Program must also include reasonable, industry-standard security practices. Such practices must be evolved throughout the term of this Agreement consistent with the best practices within industry. Ingram Micro's CISO, in its sole discretion at the request of Supplier's CISO or POC, may permit certain exceptions to the Guidelines. Supplier will provide Ingram Micro with up-to-date contact information of its POC and CISO to Ingram Micro's Information Security Operations Center (see Exhibit B). Upon request, Supplier will make available its POC or CISO within a reasonable amount of time. At no cost to Ingram Micro, Supplier will comply with all laws and regulations

governing data, cybersecurity, and privacy. Supplier will not implement any changes that would: (i) decrease the maturity; (ii) degrade an information security Control, tool, or process; or (iii) decrease the scope or coverage of the Supplier's Cybersecurity Program or Guidelines.

**6.1. "Control."** Components, processes, and restrictions that apply to information technology to ensure the confidentiality, integrity, and availability of systems and data. Controls are derived from the Guidelines, regulations, and the [Institute of Internal Auditors](#) Global Technology Audit Guide (or a comparable standard).

**7. Third Party Compliance.** Supplier will: (i) enter into a written agreement with any Third Party who, on behalf of the Supplier has access or use of Ingram Micro Data and impose the requirements of this Agreement; (ii) enforce compliance with such written agreement; (iii) enforce such written agreement on the Third Party's workforce; and (iv) remain responsible to Ingram Micro for the actions or omissions of the Third Party's workforce, sub-contractors, or company itself with respect to the terms and conditions of this Agreement. Supplier will notify Ingram Micro in writing prior to using a Third Party to perform the services. If Ingram Micro reasonably believes at any time that a Third Party is not in compliance with this Agreement or that Supplier's use of such Third Party poses a conflict with Ingram Micro's business, Ingram Micro may object to the use of the Third Party and Supplier has no more than **%%%** (%%%) business days or as otherwise permitted by Ingram Micro's CISO to replace the Third Party without degrading the services provided to Ingram Micro. Supplier may never sell, rent, or lease Ingram Micro Data to any individual, organization, or Third Party.

**8. Data Protection and Privacy.** If Supplier is provided access to Personal Data, Supplier agrees to maintain an appropriate data protection and privacy program in compliance with local, state, federal and international laws, including, but not limited to, the European Union General Data Protection Regulation, California Consumer Privacy Act, and Brazil's General Data Protection Law. Depending on the scope of the Personal Data provided to Supplier, Ingram Micro may require Supplier enter into a Data Processing Agreement, which may be made an exhibit to this Agreement or another agreement between the Parties.

**9. Cybersecurity Compliance Programs.** Supplier will commission an annual external audit and provide a copy of the results with Supplier's annual attestation for the following compliance programs, the scope of which must include all systems, processes, and personnel pertaining to Ingram Micro (list applicable):

**General Security**

- ISO/IEC 27001
- ISO/IEC 28000
- SOC 1 Type 2
- SOC 2 Type 2
- O-TTPS

**Privacy**

- ISO/IEC 27018
- ISO/IEC 27701
- GDPR
- CCPA/CPRA
- LGPD
- PIPEDA
- HIPAA

**Public Sector**

- FedRAMP
- FAR/DARS
- SPRS

**Other**

- PCI-DSS
- PA-DSS

**Cloud**

- ISO/IEC 27017
- Cloud Security Alliance STAR

**10. Security Events and Incidents.** Supplier will report all Security Incidents within 24 hours of Discovery to Ingram Micro by emailing and calling Ingram Micro's Information Security Operations Center (see Exhibit B). Supplier will make its POC, delegate, or security operations center, available to Ingram Micro personnel **%%%** hours per day, **%%%** days per year, without limitation. Supplier POC will respond to an Ingram Micro contact within **%%%** minutes with appropriate personnel who are capable and competent to handle a Security Event or Incident.

**10.1. Remediation for Breach of Sensitive Data.** With regard to Personal Data governed by laws or regulations, Supplier will provide Ingram Micro with a list of all affected individuals within thirty-six (36) hours from the time such Breach is Discovered. If Ingram Micro determines that the Breach triggers remediation requirements under any applicable law or regulation, then Supplier must promptly remediate all affected individuals based on the most stringent regulatory requirements. Supplier will provide a remediation plan to Ingram Micro for review and approval. The remediation plan must be fully executed by the Supplier

within %%% business days of the Discovery of the Breach. Supplier must arrange and administer a toll-free telephone number and provide a call center to assist affected individuals in understanding the circumstances of the Breach and the remedies available to them. Supplier will engage an identity theft monitoring company acceptable to Ingram Micro and which provides a minimum of %%% (from the date of Breach) of full identify monitoring and credit restoration services to all affected individuals.

**10.2. Cooperation with Law Enforcement Investigations.** Supplier agrees to coordinate and cooperate with Ingram Micro as to any law enforcement inquiry into, investigation with or other involvement in a Security Incident, except where such coordination or cooperation with Ingram Micro would violate applicable law.

**11. Reporting.** Supplier will provide Ingram Micro with a complete and thorough annual attestation, in the form provided on the attached Exhibit A (the "**Attestation**"), affirming Supplier's compliance with the Guidelines.

**12. Auditing.** Ingram Micro will have the right to audit Supplier's use of the Ingram Micro Data to assure compliance with the terms of this Agreement and applicable laws. Supplier agrees to provide Ingram Micro full cooperation in connection with such audits and will provide Ingram Micro access to such properties, records, and personnel as Ingram Micro may reasonably require for such purpose.

**13. Testing.** Supplier will perform annual penetration testing and monthly vulnerability testing on its internet perimeter network in compliance with the Guidelines or materially equivalent standards, using industry standard security tools and qualified cybersecurity experts. On an annual basis, Supplier will submit its testing methodology and results to Ingram Micro upon request. After giving Supplier %%% business days' notice, Ingram Micro may also perform its own penetration testing or vulnerability testing of Supplier's external perimeter network. Supplier will not block or otherwise impede the ability of Ingram Micro to complete its testing.

**13.1. Remediation.** Supplier agrees to remedy any deficiencies, weaknesses, non-compliance, or non-conformance with Guidelines with a commercially reasonable amount of time. Supplier will provide Ingram Micro with an estimated time for remediation within %%% business days. Supplier will notify Ingram Micro upon completion of remediation actions.

**14. Insurance.**

**14.1. Requirements of all Policies**

- a) Prior to performance of the Services and the entry of any of its goods, employees, suppliers, subcontractors, or agents into any Ingram Micro facility as permitted under this Agreement, Supplier will, at its own expense, at all times during the term of this Agreement provide and maintain in effect those insurance policies and limits of coverage as set forth below and any other insurance required by law in any country, state, nation or territory where Supplier provides Services under this Agreement, with insurance companies with an A.M. Best's Insurance Rating of A:VIII or better or as otherwise acceptable to Ingram Micro, and will comply with all those requirements as stated herein. In no way do these requirements limit the liability assumed elsewhere in this Agreement, including but not limited to Supplier's defense and indemnity obligations.
- b) Supplier's insurance will be primary to and noncontributory with all other insurance maintained or otherwise afforded to Ingram Micro, its officers, directors, employees and agents.
- c) Supplier's insurance will include Ingram Micro, its subsidiaries and affiliates, and their respective officers, directors, shareholders, employees, and agents as additional insureds to the extent their interests may appear on their General Liability, Automobile Liability, Umbrella Liability, and Professional Liability insurance policies.
- d) Except where prohibited by law and the required Crime Insurance, Supplier and its respective insurers waive all rights of recovery or subrogation against Ingram Micro, its officers, directors, employees, agents, and insurers.
- e) In the event Supplier uses the services of subcontractors to perform the Services contemplated hereunder, Supplier will require from or provide for all subcontractors the same insurance requirements detailed below.

- f) If an insurance policy required under this Agreement is written on a claims-made basis, then Supplier will continue to maintain such insurance for %%% years following completion of and acceptance of the Services by Ingram Micro.

**14.2. Required Insurance Coverage**

- a) **Workers' Compensation Insurance.** Supplier will carry Workers' Compensation insurance as required by, and in accordance with the provisions of, any applicable law or regulation of the nation, state, territory or province having jurisdiction over Supplier's employees. Employer's Liability insurance will be provided with a limit of %%%.
- b) **Commercial General Liability Insurance.** Supplier will carry Commercial General Liability insurance covering all operations by or on behalf of Supplier arising out of or connected with this Agreement providing insurance for bodily injury, property damage, personal injury and advertising injury and contractual liability, as those terms are defined by Commercial General Liability insurance policies, with a limit of %%% each occurrence and %%% in the aggregate.
- c) **Automobile Liability Insurance.** If Supplier will be onsite at any Ingram facility at any point in time, then Supplier will carry Comprehensive Business Automobile Liability insurance, including bodily injury and property damage for vehicles with limits not less than those required by law, regulation, or statute where services are to be provided hereunder or %%%, whichever is greater.
- d) **Umbrella/Excess Liability Insurance.** Supplier will carry Umbrella Liability and/or Excess Liability insurance with a limit of %%% per occurrence in excess of the limits provided by the Employer's Liability, Commercial General Liability, and Automobile Liability insurance policies. Such insurance must provide for contractual liability coverage, and cross liability coverage.
- e) **Professional Liability (Errors & Omissions) Insurance.** If Supplier will provide professional services and/or technology products, then Supplier will carry insurance for professional liability, including but not limited to coverage for errors and omissions in the performance of professional services under this Agreement, with a limit of %%% per occurrence or per claim and %%% in the annual aggregate.
- f) **Cyber Risk (E-Commerce or Internet Security) Insurance.** If Supplier will provide professional services and/or technology products, then Supplier will carry insurance for e-commerce that covers the following risks: (a) liability arising from theft, dissemination and/or use of Confidential Information stored or transmitted in electronic form, and (b) liability arising from the introduction of a computer virus into, or otherwise causing damage to, a customer's or third person's computer, computer system, network or similar computer-related property and the data, software and programs stored thereon. Such insurance will be maintained with a limit of %%% per occurrence or per claim.
- g) **Crime (Fidelity) Insurance.** If the Supplier will have access to or will be handling money, securities, bank account information, customer account information or similar sensitive information, Supplier will carry insurance for loss or damage arising out of or in connection with any fraudulent, dishonest or unauthorized acts, including but not limited to forgery or alteration of documents or computer records, committed by the employees or subcontractors of Supplier, whether acting alone or in collusion with others, including but not limited to the property, funds, or negotiable instruments of others with a limit of %%%.

**14.3. Certificates of Insurance**

- a) Within %%% days after signing this Agreement and after renewal or replacement of coverage for the duration of the Agreement, Supplier will provide Ingram Micro with Certificates of Insurance (COI) evidencing the required coverage.
- b) Such certificates will specifically confirm Ingram Micro's primary and non-contributory status, additional insured status, and the required waiver of subrogation. Supplier's failure to provide certificate of insurance in compliance with the insurance requirements herein, or Ingram's failure to receive certificates, will not limit or relieve Supplier of its obligation to comply with the requirements set forth above or constitute a waiver of the requirements herein.

- c) The COI will include the following language in the DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES section:

*This insurance will be **primary and non-contributory**. Ingram Micro is named as an **additional insured** with respect to General Liability, Auto Liability, Umbrella Liability, and Professional Liability. Workers' Compensation, General Liability, Auto Liability, Umbrella Liability, Professional Liability and Cyber Liability will contain a **waiver of subrogation** in favor of Ingram Micro.*

- d) The COI will name Ingram Micro as the certificate holder:

Ingram Micro, Inc.  
3351 Michelson Drive, Suite 100  
Irvine, California 92612

**15. Liability.** No limitation or liability or liability cap contained in any agreements between Ingram Micro and Supplier will apply to a breach of the obligations arising under this Agreement.

**16. Indemnification.** Supplier will indemnify, defend and hold Ingram Micro, its Affiliated Companies, and their respective officers, directors, employees, agents, representatives, successors and assigns, harmless from and against any and all claims and demands brought by third parties and all losses, liabilities, costs and expenses, including attorneys' fees and in-house counsel fees arising from such claims and demands to the extent arising from or alleged to arise from a breach of this Agreement by Supplier, its Affiliated Companies, or their respective officers, directors, employees, agents, or representatives or from acts or omissions of any such parties in breach of this Agreement relating to the Ingram Micro Data. Supplier will defend any claim at its expense and pay all settlements preapproved by Ingram Micro in writing and any judgments which are finally awarded, provided that, Ingram Micro allows Supplier to control the defense of such claim (subject to the right of Ingram Micro to hire counsel at its own expense to assist in the defense of the claim) and cooperates reasonably in such defense.

**17. Injunctive Relief.** Supplier acknowledges that monetary damages may not be a sufficient remedy for unauthorized disclosure or use of Ingram Micro Data or any other breach of this Agreement and agrees that Ingram Micro will be entitled, without waiving any other rights or remedies nor being required to post any bond, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

**18. Investigations.** When appropriate, Supplier will conduct a digital forensic investigation of a Security Incident and provide Ingram Micro with its findings and reports. At Ingram Micro's request, Supplier will provide to Ingram Micro forensic copies of any evidence collected during the Supplier's investigation. Supplier also agrees to cooperate with Ingram Micro if Ingram Micro also elects to perform an investigation of a Security Incident, including providing full access to systems, networks, and data potentially affected by the Security Incident. Supplier will resolve material risks identified by an investigation in accordance with the requirements in Section 10.1 "Remediation".

**19. Electronic Discovery.** If Ingram Micro requires Ingram Micro Data to be preserved or produced in electronic format from Supplier in connection with a discovery process, lawful search warrant, court order, subpoena or other valid legal process, then Supplier must promptly make all commercially reasonable efforts to meet Ingram Micro's requirements.

**20. Disclosure Pursuant to Legal Process.** Supplier must promptly notify Ingram Micro by sending an email and calling Ingram Micro's Chief Information Security Officer (CISO) (see Exhibit B) if Supplier is requested or required by law, court order, warrant, subpoena, or other legal or judicial process to disclose any Ingram Micro data to any third party, so that Ingram Micro may first have the opportunity to seek a protective order, confidential treatment, or other appropriate remedy to such request or requirement. Supplier must provide Ingram Micro with all reasonable assistance in opposing any required disclosure or seeking a protective order or confidential treatment for all or part of such Ingram Micro Data. Supplier may disclose only such Ingram Micro Data as is required by the court, tribunal, governmental agency or other authority, subject to any protective order or confidential treatment obtained by Ingram Micro.

**21. Service Level Agreements.**

**21.1. "Penalty Amount"** will be %%% percent (%%%) of average annual spend of Ingram Micro to the Supplier over the past one (1) year, including the current year's actual and reasonably predicted future spend.

**21.2. Failure to Report a Security Incident.** Supplier will credit or repay Ingram Micro the Penalty Amount when Supplier fails to notify Ingram Micro of a Security Incident or notification exceeds %%% hours after Discovery.

**21.3. Failure to Submit an Annual Attestation.** Supplier will credit or repay Ingram Micro the Penalty Amount when Supplier fails to provide Ingram Micro with a completed annual attestation: (i) within %%% days of a written request by Ingram Micro to Supplier's CISO and POC using the email address submitted by Supplier in Ingram Micro's supplier portal; and (ii) after twelve (12) months have elapsed since the last annual attestation.

**21.4. Failure to Remediate a deficiency, weaknesses, non-compliance, or non-conformance.** Supplier will credit or repay Ingram Micro with Penalty Amount when Supplier fails to remediate a deficiency within the time frame required in the Agreement plus %%% (%%%) calendar days.

**21.5. Failure to Complete Annual Security Training.** Supplier will credit or repay Ingram Micro with Penalty Amount when Supplier's users fail to complete annual Information Security training by the deadline plus %%% (%%%) calendar days.

**22. Breach.** If Supplier violates any of the terms, conditions, requirements, or policies within this Agreement, Ingram Micro may terminate any agreement between the parties for cause by written notice. Such termination will occur at no cost to Ingram Micro. Supplier will participate, at no cost to Ingram Micro, in executing a proper transition plan to a new supplier.

**23. Term: Termination.** This Agreement shall be effective until it is terminated or expires according to the provisions stated herein. Either Party may terminate this Agreement for convenience upon %%% days prior written notice and will not have to pay the other Party any compensation, costs or damages resulting from the termination of this Agreement without cause. Either Party may terminate this Agreement if the other Party: (a) materially breaches any term of this Agreement and fails to cure the breach within the applicable cure period or %%% days after written notification if no cure period is specified in this Agreement; (b) ceases to conduct business in the normal course; or (c) becomes insolvent, makes a general assignment for the benefit of creditors, suffers or permits the appointment of a receiver for its business or assets, or avails itself of or becomes subject to any proceeding under any applicable bankruptcy or insolvency law. The rights and obligations of Supplier with respect to the security and confidentiality of Ingram Micro Data will survive until such time as Supplier no longer holds any Ingram Micro Data and such other provisions of this Agreement that are intended to survive the Term of this agreement will survive expiration or termination including but not limited to Confidentiality, Insurance and Indemnification.

**24. General Terms.** This Agreement constitutes the entire agreement between the Parties regarding its subject matter. This Agreement supersedes and terminates any and all previous proposals, representations or statements, oral or written. In the event of a conflict in the terms and conditions contained in each party's purchase orders, invoices, acknowledgments, confirmations, agreements, contracts, or similar documents and this Agreement, the provision imposing the stricter requirements will control. Any modifications to this Agreement must be in writing and signed by authorized representatives of both Parties. This Agreement may be executed in one or more counterparts, each of which will be considered an original, but all of which together will constitute one and the same instrument. Delivery of an executed counterpart of this Agreement by facsimile or electronic copy will be as effective as delivery of the original version. Unless a provision setting forth the rights or obligations of a Party is expressly terminated as set forth in the specific language of the provision, the Parties agree that all rights and obligations set forth in this Agreement, which by their nature or operation are considered material, will survive expiration or termination of this Agreement (e.g., nondisclosure, indemnification, limitation of liability, warranties, etc.). Supplier may not and will not attempt to assign this Agreement or delegate its obligations without the express written consent of Ingram Micro. This Agreement is binding upon and will inure to the benefit of the Parties hereto and their respective successors and permitted assigns. The waiver by either Party of a breach of any provision of this Agreement will not be a waiver of the provision itself or a waiver of any breach in the future, or a waiver of any other provision in this Agreement. Failure to require performance will not affect a Party's right to require performance of that or any future duty. If any provision in this Agreement is held to be invalid, illegal or unenforceable, that provision will be enforced to the fullest extent permitted by

applicable law and the validity, legality and enforceability of the remaining provisions will not in any way be affected or impaired so long as the economic or legal substance of the transactions contemplated by this Agreement is not affected in any matter materially adverse to any Party. All attachments, documents, and exhibits referenced in this Agreement or attached to this Agreement, if any, are an integral part of this Agreement. In the event of any conflict between the terms and conditions of any exhibits, documents, and this Agreement, the terms of this Agreement will control unless otherwise agreed to in writing by authorized representatives of the Parties. All legal notices sent by one Party to the other must be in writing and sent to an authorized representative of the Party at the address set forth below the signature block (or other address as the Parties may designate including the email address of that authorized representative), and may be: (i) personally delivered to an officer of the other Party or if a Party is an individual person, to that person; or (ii) sent by registered or certified mail, return receipt requested, or by any nationally recognized courier service. For the purposes of notices to Ingram Micro, notices will be addressed to both "Legal Department" and "CISO". Each Party represents and warrants that its signatory of this Agreement is an authorized representative.

**IN WITNESS WHEREOF**, the Parties hereto have executed this Agreement effective as of the Effective Date on the date(s) set forth below.

Ingram Micro Inc.	[company name]
X _____	X _____
Name: Forrest Smith	Name:
Title: CISO	Title:
Address: 3351 Michelson Suite 100	Address:
Irvine CA 92612	
Date:	Date:
Email: %%%@ingrammicro.com	Email:
Phone: 1-%%-%-%	Phone:



Supplier to complete an annual attestation every year on the contract anniversary based on the Agreement Effective Date and the agreed upon terms. The annual attestation will be completed using the supplier portal.

1. Supplier has complied with the terms and conditions of the Agreement between [start date] and [end date], except as noted below:
  - a)
  - b)
  - c)
2. During the previous year, all Security Incidents have been reported to Ingram Micro as required by the terms and conditions of the Agreement, except for the following incidents:
  - a)
  - b)
  - c)
3. During the previous year, all changes to the Cybersecurity Program have been reported to Ingram Micro as required by the terms and conditions of the Agreement, except for the following:
  - a)
  - b)
  - c)
4. \_\_\_\_ (number of users) computer and network users at Supplier have completed an annual information security training course within the previous %%% months \_\_\_\_ (number of users) have not.
5. An annual penetration test and monthly vulnerability tests have been performed on the external internet facing perimeter of Supplier's network. All deficiencies have been corrected, except the following issues:
  - a)
  - b)
  - c)

1. Certificates of Insurance: certificates must expressly confirm at least the agreed upon coverages and endorsements as set forth in the Agreement.
2. Certificate of Compliance for the Cybersecurity Compliance Program certifications agreed to above.
3. Annual Information Security Course Contents.

[company name]	
X	
Name:	
Address:	
Date:	
Email:	
Phone:	

## Exhibit B – Contacting Ingram Micro’s Information Security Team

Information Security Operations Center (“SOC”)		
	Email	%%%% @ingrammicro.com
	Web	%%%%
	Phone	%%%% United States, Toll-Free
		%%%% United States
		%%%% India, Toll-Free
		%%%% Mexico, Toluca, MEX
		%%%% United Kingdom, Toll-Free
		%%%% New Zealand, Toll-Free
		%%%% Bulgaria
		%%%% Columbia
		%%%% Hong Kong, Toll-Free
		%%%% Australia, Toll-Free
		%%%% Sweden, Toll-Free
		%%%% Singapore, Toll-Free
		%%%% Brazil, Toll-Free
		%%%% Chile
		%%%% Hungary
		%%%% Belgium, Toll-Free
		%%%% Austria, Toll-Free
		%%%% Poland, Warsaw
		%%%% Spain, Toll-Free
Chief Information Security Officer		
	Email	%%%% @ingrammicro.com
	Phone	%%%% (voice and text message)