# DATA SECURITY ADDENDUM

The following Data Security Addendum (this "**Addendum**") is not intended to be an all-inclusive list of security services and obligations necessary to comply with Security Best Practices, but is intended to capture key elements of such a program. Michaels reserves the right to amend, revise, modify, cancel and/or reissue this Addendum and will make any such amended, revised, modified and/or reissued version available on its website at www.michaels.com/supplier-portal.

**1.** As used in this Addendum, the terms set forth in this Section 1 will have the meanings provided herein. All other terms capitalized but not defined herein shall have the respective meanings assigned to them in the Terms.

"**PII**" means personally identifiable information of employees or customers of Michaels or its Affiliates, including name, address, phone number, e-mail address, date of birth, social security number, credit card information, driver's license number, account numbers, PINs and/or passwords, and any other information that could reasonably identify a person or household or "personally identifiable information," "personal data" or "personal information" under any privacy or data security law in any jurisdiction applicable to the processing of such personal information.

"**Security Policies**" means statements of direction for securing company information pertaining to Security Best Practices and mandating compliance with applicable laws and regulations. Typically, Security Policies are high level instructions to management on how the organization is to be run with respect to Security Best Practices.

"**Security Procedures"** means statements of the step-by-step actions taken to achieve and maintain compliance with Security Best Practices.

"**Security Technical Controls**" means any specific hardware, software or administrative mechanisms necessary to enforce Security Best Practices in accordance with the Terms as methods for addressing security risks to information technology systems and relevant physical locations, or implementing related policies. Security Technical Controls specify technologies, methodologies, implementation procedures, and other detailed factors or other processes to be used to implement Security Policy elements relevant to specific groups, individuals, or technologies.

**2.** To the extent that Vendor will have access to any Confidential Information, and/or data containing PII, the following section applies:

(a) Vendor shall provide a secure environment for all of Michaels' Confidential Information and/or PII, and any hardware and software (including servers, network and data components) to be provided or used by Vendor as part of its performance under this The Terms. Vendor represents that the security measures it takes in performance of its obligations under the Terms are, and will at all times remain, at the highest of the following (collectively referred to herein as "**Security Best Practices**"): (i) Privacy & IT Security Best Practices (as defined by ISO27002); (ii) the security requirements, obligations, specifications and event reporting procedures set forth in this Addendum; (iii) if applicable, maintain Payment Card Industry Data Security Standard v. 1.2 or better (so as to be classified as a Level 1 Service Provider) compliance continuously during the term of this The Terms as required by applicable rules of credit card

associations; and (iv) any security requirements, obligations, Specifications and/or event reporting procedures set forth in the applicable Statement of Work. Vendor shall contractually require any subcontractors or agents with access to Michaels' Confidential Information to adhere to such Security Best Practices.

(b) Michaels (or its designated representatives) shall have the right on an annual basis or more frequently as reasonably requested by Michaels, at Michaels' expense, to conduct an audit to verify that Vendor is operating in accordance with Security Best Practices. Such audit may include a review of all aspects of Vendor's performance hereunder, including, but not limited to: (i) network, operating system, database and application configuration controls; (ii) general controls and security practices and procedures; (iii) disaster recovery and back-up procedures; (iv) change and problem management processes and procedures; (v) invoice processing; (vi) service level compliance; (vii) network and system vulnerability and risk analysis; and (viii) resource consumption. Vendor will cooperate with Michaels in conducting any such audit, and shall allow Michaels reasonable access, during normal business hours and upon reasonable notice, to all pertinent records, documentation, computer systems, data, personnel and processing areas as Michaels deems necessary to accurately and effectively complete such audit. Michaels will take reasonable steps to ensure that such audit will not materially impact Vendor's business or operations. Vendor shall promptly correct any deviations from Security Best Practices that are identified in any security audit.

(c) Vendor will immediately notify Michaels, in writing, upon the discovery of a security incident, breach, or unauthorized use or disclosure (a "**Breach**") of Michaels Confidential Information or PII, or any Breach within Vendor's own infrastructure which affects or might affect Michaels' infrastructure, data, or systems. Vendor will coordinate with Michaels to determine additional specific actions that will be required of Vendor for mitigation of the Breach, which may include notification to affected parties, and provide timely updates of all remediation activities. All associated costs shall be borne by Vendor. Within seven (7) days of the closure of the incident, Vendor will provide Michaels with a written report describing the incident, actions taken and plans for future actions to prevent a similar incident.

**3. Information Security Policy.** Vendor specifically represents and warrants that it has established and during the Duration it will at all times enforce:

(a) an ongoing program of Security Policies, Security Procedures, and Security Technical Controls;

(b) a security incident management program;

(c) a security awareness program;

(d) business continuity and recovery plans, including regular testing;

(e) rigorous change control procedures; and

(f) procedures to conduct periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities,

and provide for timely remediation.

**4.** **Physical Access.** Vendor specifically represents and warrants that it has established and during the Duration it will at all times enforce:

(a) physical protection mechanisms for all information assets and information technology to ensure such assets and technology are stored and protected in appropriate data centers;

(b) appropriate facility entry controls are in place to limit physical access to systems that store or process data;

(c) processes to ensure access to facilities is monitored and is restricted on a "need to know" basis; and

(d) controls to physically secure all Confidential Information and to properly destroy such information when it is no longer needed;

**5.** **Logical Access.** Vendor specifically represents and warrants that it has established and during the Duration it will at all times enforce:

(a) appropriate mechanisms for user authentication and authorization in accordance with a "need to know" policy;

(b) controls to enforce rigorous access restrictions for remote users, contractors and service providers;

(c) timely and accurate administration of user account and authentication management;

(d) processes to ensure assignment of unique IDs to each person with computer access;

(e) processes to ensure vendor-supplied defaults for passwords and security parameters are changed and appropriately managed ongoing;

(f) mechanisms to track all access to Confidential Information by unique ID;

(g) mechanisms to encrypt or hash all passwords; and

(h) processes to immediately revoke accesses of inactive accounts or terminated/transferred users.

**6.** **Security Architecture and Design.** Vendor specifically represents and warrants that it has established and during the Duration it will at all times maintain:

(a) a security architecture that reasonably assures delivery of Security Best Practices;

(b) documented and enforced technology configuration standards;

(c) processes to encrypt Confidential Information in transmission and storage;

(d) processes to ensure regular testing of security systems and processes;

(e) a system of effective firewall(s) and intrusion detection technologies necessary to protect Confidential Information; and

(f) database and application layer design processes that ensure web site applications are designed to protect the information data that is collected, processed, and transmitted through such systems.

**7. System and Network Management.** Vendor specifically represents and warrants that it has established and during the Duration it will at all times maintain:

(a) mechanisms to keep security patches current;

(b) processes to monitor, analyze, and respond to security alerts;

(c) appropriate network security design elements that provide for segregation of data;

(d) use and regular update anti-virus software; and

(e) processes to regularly verify the integrity of installed software.

**7. Privacy.** Vendor specifically represents and warrants that it has established and during the Duration it will at all times maintain a privacy program that protects the privacy of PII as prescribed by the applicable privacy laws and regulations, declarations, decrees, directives, statutes, or other enactments, orders, mandates or resolution issued or enacted by any government entity (including any domestic or foreign, supra-national, state, county, municipal, local, territorial or other government).

* * *