BMC INFORMATION SECURITY REQUIREMENTS

Revised: August 2, 2023

These Information Security Requirements ("**Information Security Requirements**") form part of the Master Services Agreement (or other written agreement) entered between BMC and Company for the subscription and/or purchase of Services and/or products by BMC, as such Services are described in the corresponding Order(s) and/or Statement of Work(s) attached to such Agreement(s) (collectively the "**Agreement(s)**"). Company and BMC may be referred to individually as a "**Party**" or collectively as the "**Parties**".

The following sets forth BMC's minimum information security program and infrastructure policies (that Company must meet and maintain in order to protect BMC Data from unauthorized use, access, disclosure, theft, manipulation, reproduction and/or possible Security Breach during the provision of Services under the Agreement and for any period of time thereafter during which Company has possession of or access to BMC Data. Capitalized terms used but not otherwise defined herein have the respective meanings given in the Agreement.

1. DEFINITIONS

(a) "**BMC Data**" shall mean any files, documents, code, plans, data, or information provided or made available by BMC or on behalf of BMC to the Company during the term of the Agreement.

(b) "**Security Breach**" shall mean any actual or attempted acquisition of or access to BMC Data by an unauthorized person that compromises the security, confidentiality, or integrity of such BMC Data which was developed, maintained, processed, or transmitted by Company, its agents, or subcontractors in connection with the Services. "Security Breach" shall also be deemed to include any breach of security, confidentiality, or privacy as defined by any applicable law, rule, regulation, or order.

2. SECURITY POLICY

(a) Company has a published and enforced Information Security Policy communicated to all employees, contractors, workers, and third parties. The policy specifies practices for acceptable use of computing resources, data, and punitive actions when policies are not followed.

(b) Upon request, evidence of the above Information Security Policy will be provided to BMC for review.

(c) Company has personnel in a security role. The security role is not compromised if overlapping with operational or engineering roles that manage the applications, hosts, and other infrastructure used to process, store, or host BMC Data and assets. Company attests that appropriate due care and due diligence are being exercised to ensure the confidentiality, availability, and integrity of BMC Data and applications.

(d) Company shall adhere to information security best practices and implement Information Security controls as set out in International Organization for Standardization 27002 and/or NIST 800-53.

(e) Information security policies, procedures, standards and other security and privacy best practices shall be documented and kept current regarding changes in applicable law and industry standards.

(f) Company has a published acceptable use policy for all assets used in the provisioning of Services to BMC.

(g) Company has appropriate third-party contractual agreements in place and complies with applicable legal requirements to ensure the provisions of this Exhibit. Company maintains appropriate safeguards and service delivery levels for subcontracted services.

3. ORGANIZATION OF INFORMATION SECURITY

(a) Company has an information security function responsible for industry accepted information security practices.

(b) Company's information security function is responsible for coordinating information security activities as incident and breach response, third party access, and setting security best practices.

4. HUMAN RESOURCES SECURITY

(a) If applicable, and as permitted by applicable law, Company attests that Company's employees and all its subcontractors who are engaged in provision of Services to BMC have complied with all applicable background verification, criminal record check, and other pre-employment screening to all employment candidates, contractors, and third parties in accordance with requirements set forth in the Agreement.

(b) Company maintains Confidentiality, Non-Disclosure Agreements, and similar agreements for all employees, contractors, and third parties.

(c) Company removes access rights for all employees, contractors, third parties, and other workers to information processing facilities and BMC Data immediately upon worker termination.

(d) Company ensures that each Company employee completes Company's Code of Conduct training which governs appropriate use of technology and data and requires acknowledgement that he or she has been trained and shall comply with the requirements of Company's information security safeguards; and Company certifies to each of the foregoing.

(e) Company provides or requires periodic, no less frequently than annually, security awareness and operational training to/from all employees, contractors, subcontractors and third parties.

5. ACCOUNT AND PASSWORD MANAGEMENT

(a) Company provides a means to force periodic password changes for Company employees and all subcontractors.

(b) Company enforces a password management policy for Company employees and all subcontractors consistent with ISO 27002 and/or NIST 800-53. If Company follows ISO 27002 requirements, the following provisions shall apply:

i. Passwords change within 90 days
ii. Reuse of last 10 passwords is prohibited
iii. Account lock out after no more than 10 consecutive failed authentication attempts
iv. Password length of at least eight characters
A. Required inclusion of a combination of 3 of 4-character types:
- Lower case
- Upper case
- Numbers
- Special characters

6. AUTHORIZATION AND ACCESS CONTROLS

(a) Company shall limit access to BMC Data to those employees, authorized agents, contractors, consultants, service providers, and subcontractors who have a need to access such data in connection to the uses permitted by this Agreement ("**Authorized Persons**").

(b) Company ensures that each Authorized Person: (a) is advised of and complies with the provisions of this Agreement regarding the privacy and security of BMC Data; (b) is trained regarding their handling of all BMC Data including but not limited to customer data; and (c) accesses the data only for the purposes for which the access was granted. Company shall re-evaluate its list of Authorized Persons at least quarterly.

(c) Company is responsible for any failure of its employees, agents, subcontractors and any authorized third party to comply with these terms and conditions regarding BMC Data.

(d) Company agrees to abide by the principle of least privilege when assigning access to resources containing BMC assets or used to manage BMC assets.

(e) Company will perform monthly reviews for all administrative access used to support infrastructure and applications used to host BMC Data or provide Services to BMC.

(f) Segregation of duties is used to ensure separation of privileged access requestors from approvers.

(g) Company shall use multi-factor authentication (MFA) and company-managed devices to access its resources remotely.

7. SYSTEMS DEVELOPMENT

(a) Company ensures that source code and similar configuration changes are properly authorized and tracked via standard source code management practices.

(b) Company uses a documented, repeatable practice for testing, requesting, approving, and implementing system changes.

(c) Company performs system, user, and acceptance testing of content and infrastructure for the BMC hosted applications in a development and testing environment separately from production.

(d) Confidential BMC test data are adequately protected, controlled and removed from environments used for development and testing.

(e) Company supervises and monitors outsourced software development. Third parties meet the same code management practices applied by Company to protect infrastructure and applications used to host BMC Data or provide Services to BMC.

(f) Company ensures that all code deployed in support of a BMC application or managed service is free of back doors, malware, or any other inappropriate content.

8. HOST SECURITY

(a) Company has tools implemented to detect and remediate software viruses and other malware on all systems used to access, process, or host BMC applications or BMC Data.

(b) Company implements host intrusion detection/prevention services covering all infrastructures on which BMC Data and applications are stored.

(c) Company performs vulnerability assessments and operating system hardening for all platforms used to process, store, or host BMC Data.
(d) Company has implemented a security patch and vulnerability management process to make sure operating systems and applications remain at current levels. Company attests that application and operating system security patches are applied within 30 days of such patches being made available from the relevant Company.
(e) Company follows a practice of annual third-party penetration testing and application security scans of hosts and applications relating to BMC services.
(f) Company has implemented logging solution for all infrastructure and applications hosting BMC Data.
(g) Company maintains an inventory of all assets and related parties used in providing service to BMC.

9. NETWORK SECURITY

(a) Company has implemented firewalls, intrusion detection, and other network protection services in accordance with industry best practices for securing BMC managed applications, assets, and BMC Data.
(b) Company has implemented network segmentation to limit the effect of any security compromise.
(c) Company identifies all Internet facing services that are exposed and ensures they are appropriately monitored and periodically validated. Unnecessary services are identified and removed in a timely manner.
(d) Company blocks all network traffic to and from US embargoed countries.
(e) Company utilizes application firewalls for web-based applications.
(f) Company keeps network management and security staff adequately trained.
(g) Company will prevent administrative interfaces on all hosts from being accessed from outside Company network.
(h) Company will prevent access to BMC Data from non-Company issued and managed devices.
(i) Company and subcontractors implement accepted industry practices to secure remote and wireless connectivity. Practices include strong authentication and encryption.
(j) Company implements time synchronization for systems used to process, store, or host BMC Data.

10. DATA PROTECTION

(a) Company agrees to securely store or escrow all data encryption keys used in the storage or transmittal of BMC Data.
(b) Company agrees to access or store BMC Data only on Company-issued and managed devices.
(c) Company agrees to employ industry standard encryption protecting any BMC Data in storage or in transit. Web servers shall require at least Transport Layer Security (TLS) protocol version 1.2 or better.
(d) All application and infrastructure passwords will be hashed and salted.
(e) All BMC Data will be encrypted when transferred to backup storage and other portable devices. Only strong ciphers (symmetric key length at least 256 bits) will be utilized where BMC Data is encrypted for storage or transmittal.
(f) All mobile devices storing or accessing BMC Data outside of Company’s secure sites shall be encrypted.
(g) Company agrees to provide three months of notice before any BMC Data or processes supporting BMC Data crosses national borders. BMC reserves the right to terminate, with 30 days’ notice, any agreement that would allow BMC Data to be stored, managed, or otherwise made available in countries where BMC does not approve of this practice.
(h) Company will destroy all BMC Data stored on hosted infrastructure, databases, and backup storage media at the end of the engagement.
(i) BMC Data will be encrypted, using above agreed upon encryption techniques, before being moved to any other facility for any reason.
(j) Company will ensure the privacy, integrity and confidentiality of BMC Data in transport and storage through verifiable industry standard tools, education, and practices.
(k) Backup data will be immutable (meaning it should be unchangeable) and able to be deployed to servers/endpoints immediately in case of ransomware attacks or other data loss.

11. PHYSICAL ADDRESS

(a) Company enforces badge access with both photo and electronic verification with logging to both physical premises and data centers hosting BMC Data and applications.
(b) Company uses 24x7 camera monitoring monitor for facilities, data centers, and egress points.
(c) Company uses physical intrusion and fire alarms in all areas where BMC business is conducted.
(d) Company logs physical access to all facilities and data centers hosting BMC Data and applications.
(e) Company assures doors remain locked for secure areas.

12. INCIDENT MANAGEMENT AND BREACH NOTICE

(a) Company has and follows a documented Security Breach response plan. In the event of any Security Breach affecting BMC Data (including data held by entrusted third parties), an application managing BMC Data or other BMC assets under Company's control, Company agrees to notify BMC via email to soc@bmc.com and by phone call to (713) 918-7762 within 24 hours of initial detection of a Security Breach. Notwithstanding the foregoing, notification obligations for a Personal Data Breach shall be as specified in the Data Processing Addendum executed by the Parties ("**DPA**"), if applicable. For purposes of this section, "**Personal Data Breach**", if applicable, shall have the meaning set forth in the DPA.

(b) When such incident occurs, Company will designate a single point of contact within Company's organization. This point of contact will initiate and manage regular incident status calls between Company, BMC, and any other involved parties.

(c) In the event of a Security Breach, Company will engage a third party of sufficient reputation to manage the response and remediation. A third-party penetration test must be performed after corrective actions are implemented with the test results to be provided to BMC.

(d) Company monitors and identifies possible intrusions on infrastructure, applications, and services used to present BMC content.

(e) Company has similar breach notification obligations with all vendors and providers engaged by Company to host BMC Data under the Agreement.

13. BUSINESS CONTINUITY

(a) Company will backup BMC applications, data, and software on a regular basis.

(b) All supporting infrastructure for BMC applications and data are available and supported in a managed disaster recovery program. This includes but is not limited to storage capacity, processing power, points of presence, power generators, and backup power.

(c) Company's business continuity plan covers infrastructure and applications used to host BMC Data or provide services to BMC.

14. RISK ASSESSMENT AND TREATMENT

(a) Company regularly performs risk assessments for all IT infrastructure used to present, manage, or otherwise sustain BMC Data, hosted applications, or application infrastructure.

(b) Identified risks are analyzed, remediated, and documented using industry accepted risk mitigation strategies such as risk avoidance, risk reduction, risk retention, and risk transfer.

(c) Risk assessment documents are retained for risk accountability.

15. LEGAL COMPLIANCE AND SECURITY POSTURE

(a) Company certifies that its information security safeguards at all times comply with applicable laws.

(b) Company agrees to require industry accepted security safeguards for any subcontracted services and to notify BMC in writing before moving any service performance to any third party or across national boundaries.

(c) Company provides BMC with the right to audit within the scope of this document. BMC will provide Company a minimum of 30 days of notice prior to the audit.