SAAS INFORMATION SECURITY REQUIREMENTS

FOR HELIX SUBSCRIPTION SERVICES

Contents

Purpose

This document sets forth BMC's information security program and infrastructure policies in effect as of the Effective Date (the "Information Security Requirements"). BMC will comply with these Information Security Requirements during the term of the Agreement and for any period of time thereafter during which BMC has possession of or access to Customer Data.

If there is a conflict between these Information Security Requirements and the underlying Agreement, these Information Security Requirements will control.

"Security Breach" shall mean (A) any circumstance pursuant to which applicable law requires notification of such breach to be given to affected parties or other activity in response to such circumstance; or (B) any actual or, attempted, compromise of, either physical security or systems security in a fashion that unauthorized processing, use, disclosure or acquisition of or access to Customer Data developed, maintained, processed or transmitted by BMC or its agents or subcontractors in connection with the Subscription Services.

Capitalized terms used but not otherwise defined in these Information Security Requirements have the respective meanings given in the Agreement.

BMC maintains a comprehensive security program to protect BMC employees, customers, assets, and data. BMC requires its subcontractors to have similar information security practices and procedures that comply with these minimum requirements to protect BMC relevant assets and data.

Security Policy

1. BMC has an Information Security Policy that it communicates to all employees, and subcontractors. The policy specifies practices for acceptable use of computing resources, data, and punitive actions when policies are not followed.
2. Upon request, evidence of BMC's Information Security Policy can be provided to Customer for review.
3. BMC has dedicated personnel in a security role. The security role does not overlap with operational or engineering roles that manage the applications, hosts, and other infrastructure used to process, store, or host Customer Data and assets. BMC uses appropriate due care and due diligence to ensure the confidentiality, availability, and integrity of Customer Data and applications.
4. BMC adheres to information security best practices as derived from National Institute of Standards and Technology Special Publication 800-53 at a Moderate baseline.
5. Information Security practices are documented and kept current based on changes in applicable law, best practices, and industry standards.
6. At least annually, at our expense, BMC has an independent certified public accounting firm conduct a review of BMC's operations and procedures related to the disaster recovery plan, Information Security, and the other material aspects of control of the Subscription Services and the system. Such review will be conducted in accordance with the AICPA's Statements on Standards for Attestation Engagements (SSAE) or any modified rules established at the time of such review. BMC will provide Customer copies of the SOC2 Type II reports of any reviews under this section within 30 days upon request by Customer. BMC will promptly address audit findings arising out of such reports within a reasonable period. In addition, if requested by Customer, BMC will provide a bridge letter to cover periods when the SOC report may be stale.
7. BMC has a published acceptable use policy for all assets used in the provisioning of Subscription Services to Customer.
8. BMC has appropriate third party contractual agreements in place and complies with applicable legal requirements to ensure the provisions of these Information Security Requirements. BMC maintains appropriate safeguards and service delivery levels for subcontracted Subscription Services.

Organization of Information Security

1. BMC has an Information Security department responsible for industry accepted information security practices.
2. This organization is responsible for coordinating Information Security activities as incident response, third party access, and setting security best practices.

Human Resources Security

1. BMC performs pre-employment background checks on all BMC employment candidates located in the US, Canada, India and China. BMC requires its subcontractors to perform background checks on its employees who are engaged in the performance of the Subscription Services, where such background checks are allowed by law.
2. BMC maintains confidentiality/non-disclosure agreements, and similar agreements with all employees and subcontractors.
3. BMC removes access rights to information processing facilities for all employees and subcontractors within 24 hours of termination.
4. BMC ensures that each BMC employee completes the BMC's Code of Conduct training on appropriate use of technology and data. BMC requires employee acknowledgement of such training and certification that each employee shall comply with BMC's Information Security Policy.
5. BMC provides security awareness and operational training to all employees and subcontractors.

Account and Password Management

1. BMC provides a means to force periodic password changes for BMC employees and all subcontractors.
2. BMC enforces a password management policy for BMC employees and all subcontractors with the following provisions:
    a. Passwords change within 90 days
    b. Reuse of last 10 passwords is prohibited
    c. Account lock out after no more than 10 consecutive failed authentication attempts
    d. Password length of at least eight characters
        i. Required inclusion of a combination of 3 of 4-character types:
            1. Lower case
            2. Upper case
            3. Numbers
            4. Special characters

Authorization and Application Controls

1. BMC limits access to Customer 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 the Agreement ("Authorized Persons").
2. BMC ensures that each Authorized Person: (a) is advised of and complies with the provisions of these Information Security Requirements and the Agreement regarding the privacy and security of Customer Data; (b) is trained regarding their handling of all data, including but not limited to Customer Data; and (c) accesses the data only for the purposes for which the access was granted. BMC re-evaluates its list of Authorized Persons at least quarterly.
3. BMC is responsible for its Authorized Persons' compliance with the terms of these Information Security Requirements regarding Customer Data.

4. BMC agrees to abide by the principle of least privilege when assigning access to resources containing BMC assets or used to manage BMC assets.
5. BMC will perform monthly reviews for all administrative access used to support infrastructure and applications used to host Customer Data or provide Subscription Services to Customer.
6. BMC uses segregation of duties to ensure separation of privileged access requestors from approvers.

Systems Development

1. BMC ensures that source code and similar configuration changes are properly authorized and tracked via standard source code management practices.
2. BMC uses a documented, repeatable practice for testing, requesting, approving, and implementing system changes.
3. BMC performs system, user, and acceptance testing of content and infrastructure for the BMC hosted applications in a development and testing environment separately from production.
4. Confidential BMC test data are adequately protected, controlled and removed from environments used for development and testing.
5. BMC supervises and monitors outsourced software development. Third parties meet the same code management practices applied by BMC to protect infrastructure and applications used to host Customer Data or provide Subscription Services to Customer.
6. BMC uses industry standard processes and technology to scan for and remove any back doors, malware, or any other inappropriate content from all code deployed in support of a BMC application or managed service.

Host Security

1. BMC has tools implemented to detect and remediate software viruses and other malware on all systems used to access, process, or host BMC applications or data.
2. BMC may implement intrusion detection/prevention services covering infrastructures on which Customer Data and applications are stored.
3. BMC performs vulnerability assessments and OS hardening for all platforms used to process, store, or host Customer Data.
4. BMC has implemented a security patch and vulnerability management process to make sure OS's and applications remain at current levels.
5. BMC follows a practice of annual third-party penetration testing and application security scans of hosts and applications relating to BMC products and services.
6. BMC implements logging solutions for all infrastructure and applications hosting Customer Data.
7. BMC maintains an inventory of all assets and related parties used in providing subscription services.

Network Security

1. BMC has implemented firewalls, intrusion detection, and other network protection services in accordance with industry best practices for securing BMC-managed applications, assets, and data.
2. BMC implements network segmentation to limit the effect of any security compromise.
3. BMC 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.
4. BMC keeps network management and security staff adequately trained.

5. BMC and its subcontractors implement accepted industry practices to secure remote and wireless connectivity. Practices include: strong authentication and encryption.
6. BMC implements time synchronization for systems used to process, store, or host Customer Data.

Data Protection

1. BMC will securely store all data encryption keys used in the storage or transmittal of Customer Data.
2. BMC will access or store Customer Data only on BMC-issued and managed devices.
3. BMC employs industry standard encryption protecting any Customer Data in transit across untrusted networks. Web servers shall support at least Transport Layer Security (TLS) protocol version 1.2 or better.
4. All stored application and infrastructure passwords will be hashed or encrypted.
5. Upon request, encryption at rest will be enabled on Customer Data.
6. If Customer Data is requested to be encrypted at rest, will also 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 Customer Data is encrypted for storage.
7. BMC will destroy all Customer Data, or the encryption keys permitting accessibility of Customer Data, stored on hosted infrastructure, databases, and backup storage media in accordance with the terms of the Agreement.
8. BMC will use verifiable industry standard tools, education, and practices to help maintain the privacy, integrity and confidentiality of Customer Data in transport and storage, as required by the terms of these Information Security Requirements and the Agreement.

Physical Access

1. BMC enforces badge access with both photo and electronic verification with logging to both physical premises and data centers hosting Customer Data and applications.
2. BMC uses 24x7 camera monitoring monitor for facilities, data centers, and egress points.
3. BMC uses physical intrusion and fire alarms in all areas where BMC business is conducted.
4. BMC logs physical access to all facilities and data centers hosting Customer Data and applications.
5. BMC maintains locked cages and/or cabinets within the secure areas of data centers where BMC hardware is hosted.

Incident Management and Breach Notice

1. BMC has and follows a documented security incident response plan. In the event of any incident affecting Customer Data or an application managing Customer Data under BMC's control, BMC agrees to notify Customer of such event consistent with the incident classification, contacts, and timing described in Attachment 1.
2. When such an incident occurs, BMC will designate a point of contact within its organization. This point of contact will initiate and manage regular incident status calls between the Customer, BMC, and any other involved parties.
3. BMC monitors and identifies possible intrusions on infrastructure, applications, and services used to present the Subscription Services.

Business Continuity

1. BMC will backup BMC applications, data, and software on a regular basis.

2. 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.
3. BMC's business continuity plan covers infrastructure and applications used to host Customer Data or provide Subscription Services to Customer.

Risk Assessment and Treatment

1. BMC regularly performs risk assessments for all IT infrastructure used to present, manage, or otherwise sustain Customer Data, hosted applications, or application infrastructure.
2. Identified risks are analyzed, remediated, and documented using industry accepted risk mitigation strategies such as risk avoidance, risk reduction, risk retention, and risk transfer.
3. Risk assessment documents are retained for risk accountability.

Legal Compliance and Security Posture

1. BMC's Information Security safeguards comply with applicable laws.
2. BMC agrees to require industry accepted security safeguards for any subcontracted Subscription Services.
3. BMC provides Customer with the right to audit within the scope of these Information Security Requirements, in accordance with the following terms:
    a. Customer and (subject to satisfactory confidentiality obligations being put in place) any of its auditors, regulators or other advisers may conduct an audit no more than once in a twelve (12) month period during the term of the Agreement ("Audit"). Unless requested otherwise by a regulator, the scope of the Audit shall be limited to: (a) NIST 800-53 and/or ISO 2700X Information Security Standards, SOC2 or equivalent; and (b) no more than three (3) days and one (1) work stream.
    b. Customer will provide 60 (sixty) days courtesy notice when Audit is required other than for cause and five (5) business days' notice when an Audit is required for cause. BMC shall provide the Customer (and its auditors, regulators and other advisers (subject to satisfactory confidentiality obligations being put in place)) with all reasonable co-operation and assistance in relation to each Audit.
    c. BMC reserves the right to not disclose information that: (a) may cause a breach of confidentiality with BMC or its other customers; or (b) could create increased risk to service security.

Attachment 1: Incident Notice Requirements

INCIDENT	CONTACT(S)	TIMING
Security Breach affecting Customer Data, systems containing Customer Data, or systems that directly interact with systems containing Customer Data, hosted and processed by BMC.	**BMC Contacts:** Via cloudsecurity@bmc.com and by phone to contacts listed in Attachment 2 and Attachment 3 **Customer Contacts:** Authorized Customer personnel as designated the Product Specific Terms for Helix Subscription Services Attachment to the Order.	Within 24 hours of confirmation of breach.

Designated Customer Contacts

Set forth on the Product Specific Terms for Helix Subscription Services Attachment to the Order

Attachment 2 - Primary Contacts

Name: BMC SaaS Security Operations Center
Email: cloudsecurity@bmc.com

Attachment 3 - Secondary Contacts

Name: Scot Shepard
Position: Sr Manager of Information Security
Location: Houston, TX
Phone: (713) 918-3334
Email: Scot_Shepard@bmc.com