Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms an integral part of the Order this DPA is attached to. Capitalized terms not defined herein have the meanings given to them in the Order or the Agreement referenced in the Order. This DPA commences on the Order Date (hereinafter referred to as the "**Effective Date**").

1. GENERAL DEFINITIONS.

1.1 "**Agreement**" is an agreed written or electronic document that sets the framework terms under which BMC Helix will supply BMC Helix Services to Customer and Customer will receive them.

1.2 "**Binding Corporate Rules**" or "**BCR**" are (i) BMC's Controller and Processor EU Binding Corporate Rules Policy, and (ii) BMC's Controller and Processor UK Binding Corporate Rules Policies, both available at www.bmc.com.

1.3 "**BMC Helix Services**" is the specific provision of Products, Subscription Services, Services and/or Support by BMC Helix to Customer agreed under an Order.

1.4 "**Customer Data**" is the Personal Data provided to BMC Helix in accordance with an Order executed by the parties.

1.5 "**Data Protection Laws**" are all applicable laws and regulations relating to the Processing of Personal Data under the Agreement, including (i) laws and regulations of the European Union, the European Economic Area and their member states, such as Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data ("**GDPR**"); and (ii) the UK Data Protection Act 2018 and the UK General Data Protection Regulation as amended or superseded from time to time ("**UK GDPR**").

1.6 "**EU SCCs**" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 of 4 June 2021. "**UK SCCs**" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner's Office. The EU SCCs and the UK SCCs are collectively referred to herein as the "**SCCs**".

1.7 "**Order**" or "**Statement of Work (SOW)**" is an agreed written or electronic document, subject to the terms of the Agreement and this DPA, that identifies the BMC Helix Services supplied by BMC Helix to Customer.

1.8 "**Personal Data**", "**Processing**", "**Controller**", "**Processor**", "**Personal Data Breach**", "**Data Protection Impact Assessment**", "**Prior Consultation**", "**Data Subject**" and "**Supervisory Authority**" have the meaning specified for each term respectively under the Data Protection Laws.

1.9 "**Third Party Controller**" means any third party Controller on behalf of whom Customer processes Personal Data.

1.10 "**Sub-processor**" means any data processor engaged by BMC Helix that processes Customer Data that may be an Affiliate of BMC Helix or a third party engaged by BMC Helix.

2. SCOPE. This DPA applies to the Processing of Customer Data in accordance with Data Protection Laws upon execution of an Order that refers to this DPA.

3. PRECEDENCE. In the event of a direct conflict between the Agreement, the terms of this DPA, and any Order, the order of precedence is: (1) the Order; (2) this DPA; (3) the Agreement, but only to the extent required to resolve such conflict.

4. TERM. This DPA commences on the Effective Date and will be in force and effect until the Order has been terminated or expires. In the event that after termination of the Order, Processing of Customer Data by BMC Helix is necessary for the purpose of the Order, the Agreement or as required by law (e.g. return of Customer Data), this DPA will continue to apply until the completion of the purpose or return, as applicable.

5. PROCESSING OF CUSTOMER DATA.

5.1 Roles of the Parties. As between the parties, Customer, as the Controller determines the purposes and means of Processing of Customer Data. BMC Helix, as the Processor, processes Customer Data on behalf of the Customer. Additionally, where the Customer, in respect of the Customer Data, is a Processor to a Third Party Controller, BMC Helix will be a Sub-processor to Customer. In that case, (a) the parties rights and obligations under this DPA may be for the ultimate benefit of the Third Party Controller and that Third Party Controller's compliance with Data Protection Law; (b) BMC Helix will cooperate and provide reasonable assistance to that Third Party Controller in the terms set forth in this DPA as if the Third Party Controller were Customer; and (c) that Third Party Controller will be entitled to exercise any rights of audit and inspection of BMC Helix in the terms set forth in this DPA as if the Third Party Controller were the Customer. Customer will be responsible for coordinating all communication with BMC Helix under this DPA and be authorized by such Third Party Controller to remit and receive any communication in connection with this DPA on behalf of its Third Party Controller. To the extent permitted by law, BMC Helix's liability arising out of or related to this DPA will be limited to Customer only, and BMC Helix will not have any liability directly to the Third Party Controller.

5.2 **Customer Processing of Customer Data**. Customer will, in connection with BMC Helix Services, process Customer Data in accordance with the requirements of Data Protection Laws. Customer's instructions for the Processing of Customer Data will comply with Data Protection Laws.

5.3 **BMC Helix Processing of Customer Data**. BMC Helix will only process Customer Data on behalf of and in accordance with Customer's documented instructions as set forth in this DPA. BMC Helix will not process Customer Data except on Customer's instructions, unless required to do so by law. Customer instructs BMC Helix to process Customer Data necessary for the exercise and performance of Customer's rights and obligations under the Agreement, the Order and this DPA respectively. Customer Data may be processed or used for another purpose only with the prior written consent of Customer. BMC Helix will immediately inform Customer if, in BMC Helix's opinion, an instruction from the Customer may infringe Data Protection Laws.

5.4 **Details of Processing.** BMC Helix will process and use Customer Data for the purposes defined in Attachment 1 to this DPA and in accordance with Customer's instructions as set forth in the Agreement, the Order and this DPA. The subject-matter, duration, nature and purpose of the processing, the types of Customer Data and categories of Data Subjects processed under this DPA are further specified in Attachment 1 to this DPA.

5.5 **Records of Processing activities**. Customer and BMC Helix will maintain records of Processing activities, in their respective roles of Controller and Processor. Parties will cooperate to fulfil the obligation to maintain such records. Any material change made by a party, requiring an update of the records of Processing activities maintained by the other party, will be notified to the other party within a reasonable time.

6. **SUB-PROCESSING**.

6.1 **Sub-processors.** Customer acknowledges and agrees that BMC Helix may engage its Affiliates or third parties as Sub-processors in connection with BMC Helix Services, including access to Customer Data. A list of all BMC Helix Affiliates acting as Sub-processors as of the Effective Date is provided in Attachment 2 to this DPA. A list of third party Sub-processors (if any) is provided in the applicable Order(s).

6.2 **Written contract.** Sub-processors will be obliged under a written contract (i) to comply with Data Protection Laws and (ii) to provide at least the same level of data protection as is required by this DPA, including the implementation of appropriate technical and organizational measures.

6.3 **Change of Sub-processors**. Any additions or replacements of Sub-processors will be notified to the Customer via email. Customer may oppose to BMC Helix use of a new Sub-processor by notifying BMC Helix in writing of its objective reasons to oppose within thirty (30) business days after receipt of BMC Helix's notice. In the event Customer objects to a new Sub-processor, BMC Helix will use reasonable efforts to make available to Customer a change in the BMC Helix Services or recommend a commercially reasonable change to Customer's configuration or use of the BMC Helix Services to avoid Processing of Customer Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If BMC Helix is unable to make available such change within a reasonable period of time, Customer may terminate the applicable Order(s) with respect only to those BMC Helix Services which cannot be provided by BMC Helix without the use of the objected-to new Sub-processor by providing written notice to BMC Helix. BMC Helix will refund Customer any prepaid fees covering the remainder of the Order term following the effective date of termination with respect to such terminated BMC Helix Services, without imposing a penalty for such termination on Customer.

6.4 **Responsibility**. BMC Helix will be liable for the performance of its Sub-processors to the same extent BMC Helix would be liable if performing the BMC Helix Services of each Sub-processor directly under the terms of this DPA.

7. **DATA SUBJECT REQUESTS**. In the event any of the parties receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject request**"), BMC Helix will do the following:

(i) If the Data Subject request is addressed to Customer, and to the extent Customer, in its use of the BMC Helix Services, cannot address it, BMC Helix will provide commercially reasonable assistance upon Customer's written request by appropriate technical and organizational measures, insofar as this is possible, and to the extent BMC Helix is legally permitted to do so, for the fulfilment of Customer's obligation to respond to a Data Subject request under Data Protection Laws; and

(ii) If the Data Subject request is addressed to BMC Helix, BMC Helix will promptly notify Customer of a Data Subject request received in connection with BMC Helix Services, to the extent legally permitted.

8. **DELETION AND RETURN**. Upon request by Customer made within forty-five (45) days after the effective date of termination of the Order(s), BMC Helix will either delete or return all the Customer Data to the Customer. After such forty-five (45) day period, if BMC Helix has not already done so, BMC Helix will delete the Customer Data from the BMC Helix Services, including copies, unless legally prohibited.

9. TRANSFER OF CUSTOMER DATA TO THIRD COUNTRIES. BMC Helix represents and Customer agrees that Customer Data subject to transfer restrictions under Data Protection Laws may be transferred to BMC Helix Affiliates in third countries, pursuant to the SCCs and the BCR. In the event of a conflict between the SCCs and the BCR, the SCCs shall prevail. If the BCR cease to apply or are no longer recognized as an appropriate safeguard, the SCCs shall be the applicable transfer mechanism. If third party Sub-processors are used, BMC Helix will transfer Customer Data to them pursuant to appropriate safeguards provided by Data Protection Laws, including SCCs.

9.1 Transfers governed by the GDPR.

By entering into this DPA, Customer and BMC Helix are deemed to have signed the EU SCCs, which form part of this DPA and shall be deemed completed as follows:

(i) Module 2 applies to transfers from Customer acting as a Controller. Module 3 applies to transfers from Customer acting as a Processor;

(ii) Clause 9(a) (Use of Sub-processors): Option 2 (General written authorization) is selected, subject to the requirements in Section 6 of this DPA;

(iii) Clause 17 (Governing law): Option 1 (law of an EU Member State) is selected. The Parties select the laws of the Netherlands;

(iv) Clause 18 (Choice of forum and jurisdiction): the Netherlands, are selected;

(v) Annex I.A (List of Parties) and I.B (Description of Transfer) are completed as set forth in Attachment 1 of this DPA;

(vi) Annex I.C (Competent Supervisory Authority): the competent supervisory authorities will be determined in accordance with Clause 13;

(vii) Annex II of (Technical and organizational measures) is completed as set forth in Attachment 3 of this DPA.

9.2 Transfers governed by the UK GDPR.

By entering into this DPA, Customer and BMC Helix are deemed to have signed the UK SCCs, which form part of this DPA and shall be deemed completed as follows:

(i) The Parties, their details and key contacts shall be as set forth in the Order Form;

(ii) The Approved EU SCCs referenced in Table 2 of the UK SCCs shall be the EU SCCs as set forth in section 9.1 of this DPA;

(iii) Either Party may end this DPA as set out in Section 19 of the UK SCCs.

10. REQUESTS FOR DISCLOSURE.

BMC Helix will ensure that where it receives a legally binding request for disclosure of Personal Data ("**Request for Disclosure**"), BMC Helix will:

(i) promptly notify the Controller, unless prohibited from doing so by a law enforcement authority or agency; put the request on hold and notify BMC Helix's competent Supervisory Authorities and the appropriate Controller's competent Supervisory Authority, unless prohibited from doing so by a law enforcement authority or agency.

(ii) If prohibited from doing so, BMC Helix will use its best efforts to inform the requesting authority or agency about its obligations under Data Protection Laws and to obtain the right to waive this prohibition.

(iii) Where such prohibition cannot be waived, BMC Helix will lawfully challenge the Request for Disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflict of laws with the laws of the European Union and/or their member states and the United Kingdom. In such case, BMC Helix will also provide the competent Supervisory Authorities with an annual report providing general information about any Requests for Disclosure it may have received from a requesting authority or agency, to the extent that BMC Helix has been authorized by said authority or agency to disclose such information.

11. SECURITY.

11.1 Confidentiality. BMC Helix will ensure that all personnel of BMC Helix granted access to Customer Data have committed themselves to confidentiality by executing written confidentiality obligations to the extent legally necessary. The obligation to treat Customer Data pursuant to such confidentiality obligations will survive the termination of the employment. Customer Data may be made available only to personnel that require access to such Customer Data for the performance of BMC Helix's contractual obligations towards Customer.

11.2 Organizational and technical protection measures. BMC Helix will maintain appropriate organizational and technical protection measures, as set out in Attachment 3 to this DPA. BMC Helix regularly monitors compliance with these measures. Upon Customer's request, BMC Helix will provide Customer with reasonable cooperation and assistance to fulfil Customer's obligation under the GDPR,

to implement and maintain appropriate organizational and technical protection measures, insofar as this obligation relates to the BMC Helix Services in scope of this DPA.

12. SECURITY BREACH MANAGEMENT, NOTIFICATION AND COOPERATION WITH AUTHORITIES.

12.1 Customer Data Breach Notification to Customer. BMC Helix will notify Customer without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data processed by BMC Helix and its Sub-processors. BMC Helix will make reasonable efforts to identify the cause of such breach and take those steps as BMC Helix deems necessary and reasonable in order to remediate the cause of such a breach to the extent the remediation is within BMC Helix's reasonable control. Where, and in so far as it is possible, the notification will:

(i) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;

(ii) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(iii) describe the likely consequences of the Personal Data Breach;

(iv) describe the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

12.2 Customer Data Breach Notification to the Supervisory Authority and the Data Subject. Upon Customer's request, BMC Helix will provide Customer with reasonable cooperation and assistance to fulfil Customer's obligation under the GDPR to notify a Customer Data Breach to the Supervisory Authority and to communicate on a Customer Data Breach to the Data Subject, insofar as this obligation relates to the BMC Helix Services in scope of this DPA.

12.3 Cooperation with Supervisory Authorities. Customer and BMC Helix will cooperate with competent Supervisory Authorities as required by the GDPR. If a party is subject to investigative or corrective powers of a Supervisory Authority, this party will inform the other party without undue delay, insofar as it relates to the data Processing covered by this DPA. Parties will provide reasonable assistance to each other to fulfil obligations to cooperate with Supervisory Authorities.

13. AUDIT AND IMPACT ASSESSMENTS.

13.1 Data Protection Impact Assessment and Prior Consultation. Upon Customer's request, BMC Helix will provide Customer with reasonable cooperation and assistance to fulfil Customer's obligation under the GDPR to carry out a Data Protection Impact Assessment related to Customer's use of the BMC Helix Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to BMC Helix. BMC Helix will provide reasonable assistance to Customer in the cooperation or Prior Consultation with the Supervisory Authority in the performance of its tasks.

13.2 Audit. Upon request by Customer, BMC Helix will make available to Customer all relevant information necessary to demonstrate compliance with this DPA, and will allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer in relation to the Processing of the Customer Data by BMC Helix and its Sub-processors. Customer will give notice of any audit or inspection to be conducted and will make reasonable endeavors to avoid causing any damage or disruption to BMC Helix premises, equipment and business while its personnel are on those premises in the course of such an audit or inspection. Any audit will be carried out on reasonable prior written notice of no less than thirty (30) days, and will not be carried out more than once a year. Access to BMC Helix premises for the purposes of such an audit or inspection is subject to: (a) the production of reasonable evidence of identity and authority by the auditors; (b) normal business hours; (c) audit personnel have committed themselves to confidentiality by executing written confidentiality obligations; and (d) access only to information that is strictly relevant to the BMC Helix Services being provided to Customer, which excludes any information relating to the provision of BMC Helix Services to other Customers. In addition to the aforementioned requirements, direct security and penetration tests require express prior written authorization from BMC Helix and compliance with the then current BMC Helix penetration tests policy.

14. LIMITATION OF LIABILITY. Each party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is exclusively subject to terms and conditions contained in the Agreement.

15. NOTICES. Notices under this DPA will be provided in writing to BMC Helix via the following email address: privacy@bmc.com.

ATTACHMENTS INCORPORATED INTO THIS DPA	
Attachment 1 – Details of Customer Data processing	X
Attachment 2 – List of BMC Helix Affiliates Sub-processors	X
Attachment 3 – Organizational and technical protection measures	X

Attachment 1 - Details of Customer Data processing

1. List of Parties

The exporter is the Customer and the importer is the BMC Helix entity, both as identified in the Order.

2. Extent, subject-matter, nature and purpose of intended processing of Customer Data

As set forth in the Agreement, BMC Helix will process Customer Data necessary for the exercise and performance of Customer's rights and obligations under the Agreement, the Order and this DPA.

Additionally, as set forth in the DPA, BMC Helix will not disclose Customer Data except as expressly permitted in writing by Customer or where required by law, in which case, to the extent legally permitted, BMC Helix will provide Customer with prior notice of any such compelled disclosure.

3. Duration of processing

The duration of Personal Data processing is the duration of the Order.

4. Categories of Customer Data and concerned Data Subjects

(a) Data Subjects

The extent of Customer data processed by BMC Helix is determined and controlled by Customer in its sole discretion. It may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer
- Customer's personnel, including Employees, agents and contractors
- Customer's Users authorized by Customer to use BMC Helix Services

(b) Categories of Personal Data

The extent of Customer data processed by BMC Helix is determined and controlled by Customer in its sole discretion. It will include Personal Data relating to the following categories of Personal Data:

- Contact details, such as name, professional phone number, professional email address, professional office address, title, degree, date of birth.
- Product usage data, such as media used, file type used, file size, usage and status and information related to BMC Helix Products such as location, language, software version, data sharing choices and update details.
- Connection data, such as number of times customer contact has engaged our Support center, duration of the engagement, means by which customer contacted BMC Helix (by email, videoconference, Support center, etc.), region, language, time zone, localization.
- Device data, such as information about Computers, and/or devices such as operating system, amount of memory, region, language, time zone, model number, first start date, age of Computer and/or device, device manufacture date, browser version, computer manufacturer, connection port, device identifiers and additional technical information that varies by Product.
- Other Personal Data provided by a Data Subject when she/he interacts, online or by phone, or mail with the Support centers, help desks and other customer support channels to facilitate delivery of BMC Helix Services and to respond to Customer or Data Subject inquiries.
- Any other Personal Data Customer or Customer's Users submit, send or store via BMC Helix Subscription Services.

Attachment 2 - List of BMC Helix Affiliates Sub-processors

The list of BMC Helix Affiliates and their jurisdictions are available at https://www.bmc.com/legal/data-privacy-binding-corporate-rules.html. This link provides names of current BMC Helix Affiliates. Any additions or replacements will be notified in accordance with Section 6.3 of this DPA. The link does not contain any other terms or conditions.

Attachment 3 - Organizational and technical protection measures

A. GENERAL ORGANIZATIONAL AND TECHNICAL MEASURES

To the extent Customer elects to provide Customer Data to BMC Helix in accordance with the relevant Order, the Agreement and this DPA, the following organizational and protection measures apply.

1. **Access control to premises, facilities and assets to prevent unauthorized persons from gaining access to data processing systems for processing or using Customer Data. BMC Helix has deployed the following measures to control access to systems and data:**

   - BMC Helix has an identity management system fully integrated with BMC Helix human resources system providing full lifecycle management for BMC Helix Users Accounts and access to data.
   - Accounts and access are revoked immediately upon termination of employment of such BMC Helix user account, including disconnection of active remote access sessions.
   - BMC Helix User Accounts are generated on a per-individual basis and not shared.
   - For BMC Helix Support, access to Support Managed File Transfer Facility ("MFT") service is restricted to authorized personnel only, which is limited to BMC Helix Support and the customer.
   - For BMC Helix Support, BMC Helix's Support MFT service is deployed in physically redundant, geographically diverse locations.
   - For BMC Helix Consulting Services, access to BMC Helix endpoints is restricted to authorized personnel only which is limited to BMC Helix Support Services and BMC Helix Consulting Services organizations.
   - BMC Helix's data centers are with industry recognized tiered providers, with:
     - Multiple certifications that may include: SSAE 16 (SOC I type II), PCI DSS (sec 9 & 12), ISO 27001, NIST
     - 24 hour security
     - Restricted, multifactor access

2. **Access control to systems to prevent data processing systems from being used without authorization.**

   BMC Helix has deployed the following measures to provide a secured access to systems:

   - BMC Helix user accounts are required in order to access BMC Helix systems. Access is restricted to authorized Support personnel, and the assigned system owner.

3. **Access control to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that Customer Data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.**

   - BMC Helix maintains a confidential information protection policy that outlines data handling practices based on classification for which all BMC Helix employees must comply.
   - BMC Helix user accounts are required to access BMC Helix systems, and are restricted to authorized Support personnel and the assigned system owner.

B. ORGANIZATIONAL AND TECHNICAL MEASURES APPLYING ONLY TO SUPPORT

1. **Disclosure control to ensure that Customer Data cannot be read, copied, altered, or removed without authorization during electronic transfer or transfer or transport or while being recorded onto data storage media, and that it is possible to check and establish to which parties Customer Data are to be transferred by means of data transmission facilities.**

   - BMC Helix has deployed security measures to ensure that Customer Data is fully encrypted, using AES 256, in transport as it moves from the Customer site to Support MFT system.
   - Customer communication to the Support MFT system requires the use of an encrypted transmission channel using Secure File Transfer Protocol (SFTP).
   - BMC Helix utilizes AES-256 encryption on disk, to ensure that data at rest on the Support MFT system cannot be read without authorization.

2. **Input control to ensure that it is possible to after-the-fact check and establish whether Customer Data has been entered into, altered, or removed from data processing systems, and if so, by whom.**

   - BMC Helix has implemented controlled and secured logging procedures applicable to the Support MFT systems where the Customer Data potentially resides.

- Logging provides full accountability for actions taken against Customer Data. Logs are retained for a period of at least a consecutive six (6) months.

3. Job control to ensure that Customer Data processed on behalf of others are processed strictly in compliance with the data controller's instructions.

- In the event Customer provides Customer Data for Support purposes, the Support MFT system provides automatic scanning of the stored data to attempt to detect data such as bank account and credit card numbers that BMC Helix does not want/need to receive.
- If BMC Helix detects data it does not want/need to receive, both the Customer and BMC Helix Support personnel are alerted so special handling or deletion procedures can be taken if needed.

4. Availability control to ensure that Customer Data are protected against accidental destruction or loss.

- BMC Helix has a 24/7 network and security operations centers (NOC/SOC) to respond to network and security related incidents and provide continuous monitoring of our systems.
- BMC Helix has a variety of security tools implemented to protect its environment and data entrusted to it, including but not limited to, intrusion prevention services (IPS), anti-virus, application heuristic analysis (sandboxing), endpoint encryption, security information and event management (SIEM), rogue system detection (RSD), and web content filtering.
- BMC Helix maintains a formal incident response and cyber crisis plan that includes standard actions and engagement for incident handling that includes notification to the Customer and authorities.

C. ORGANIZATIONAL AND TECHNICAL MEASURES APPLYING ONLY TO SUBSCRIPTION SERVICES

1. Access control to premises and facilities to prevent unauthorized persons from gaining access to data processing systems for processing or using Personal Data.

In data centers, the following measures are deployed to protect and control secured access to data center facilities:

- Access to production and disaster recovery data centers is securely controlled and monitored by industry standard layers of security.
- No entry to data center sites without approved change control, photo ID card and security center clearance.

2. Access control to systems to prevent data processing systems from being used without authorization.

The following controls are implemented:

- Unique User identifiers (User IDs) to ensure that activities can be attributed to the responsible individual.
- User passwords are stored using a one-way hashing algorithm and are never transmitted unencrypted.
- Access to the Services require a valid User ID and password combination, which are encrypted via current industry encryption standards while in transmission. Following a successful authentication, a random session ID is generated and stored in the User's browser to preserve and track session state.
- Controls to ensure generated initial passwords must be reset on first use.
- Controls to revoke access after several consecutive failed login attempts.
- Controls on the number of invalid login requests before locking out a User.
- Controls to force a User password to expire after a period of use.
- Controls to terminate a User session after a period of inactivity.
- Password history controls to limit password reuse.
- Password length controls
- Password complexity requirement.
- Verification question before resetting password.

3. **Access control to data to ensure that persons authorized to use a data processing system have access only to the data to which they have a right of access, and that Personal Data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.**

4. **Disclosure control to ensure that Personal Data cannot be read, copied, altered, or removed without authorization during electronic transfer or transfer or transport or while being recorded onto data storage media, and that it is possible to check and establish to which parties Personal Data are to be transferred by means of data transmission facilities.**

   Security measures are employed to ensure that Personal Data is fully encrypted during transmission between Customer's network and the XaaS services data centers.

   Customer communication to any XaaS services data center requires the use of an encrypted transmission channel, including at least HyperText Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS). Additional encrypted transmission channels may also include but are not limited to, Secure File Transfer Protocol (SFTP) and Internet Protocol Security Virtual Private Network (IPSec VPN).

5. **Input control to ensure that it is possible to after-the-fact check and establish whether Personal Data has been entered into, altered, or removed from data processing systems, and if so, by whom.**

   Controlled and secured logging procedures may be employed on XaaS services systems where the Personal Data resides. Logging provides full accountability for actions taken against Personal Data and by whom within the XaaS Services organization.

6. **Job control to ensure that personal data processed on behalf of others are processed strictly in compliance with the Data Controller's instructions.**

   As set forth in the DPA, BMC Helix and its Sub-processor will process Personal Data in accordance with Customer's lawful and explicit instructions, including to provide the Services as set forth in the Agreement and as instructed by Users in their use of the Services.

7. **Availability control to ensure that Personal Data are protected against accidental destruction or loss.**

   BMC Helix has a variety of security tools implemented to protect its environment and data entrusted to it, including but not limited to, intrusion prevention services (IPS), anti-virus, application heuristic analysis (sandboxing), endpoint encryption, security information and event management (SIEM), rogue system detection (RSD), and web content filtering.

   BMC Helix maintains a formal incident response and cyber crisis plan that includes standard actions and engagement for incident handling that includes notification to the customer and authorities.

   - Disaster recovery. BMC Helix or its Sub-processor may utilize disaster recovery facilities that may be geographically remote from primary data centers, along with required hardware, software, and Internet connectivity, in the event BMC Helix's Sub-processor production facilities at the primary data center were to be rendered unavailable. BMC Helix's Sub-processor has disaster recovery plans in place and tests them at least once per year.
   - Viruses. The Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Services by Customer. Any such uploaded attachments will not be executed in the Services and therefore will not damage or compromise the Services.

8. **Segregation control to ensure that data collected for different purposes can be processed separately.**

   - Permissions and access control lists within BMC Helix Subscription Services environment allow logically segregated processing of personal data;
   - Access control within the BMC Helix Subscription Services environment is restricted and isolated so usage activities for one BMC Helix customer cannot be viewed or accessed by another BMC Helix customer.

D. ORGANIZATIONAL AND TECHNICAL MEASURES APPLYING ONLY TO CONSULTING SERVICES

1. **Disclosure control to ensure that Customer Data cannot be read, copied, altered, or removed without authorization during electronic transfer or transfer or transport or while being recorded onto data storage media.**

   - BMC Helix has deployed security measures to ensure that BMC Helix Consulting Services computing systems (the PS laptops) are fully encrypted, using AES 256.
     - BMC Helix Consulting Services consultants utilize secure transmission methods for data transfer to/ from customer, such as SFTP.

2. Availability control to ensure that Customer Data are protected against accidental destruction or loss.

- BMC Helix has a 24/7 network and security operations centers (NOC/SOC) to respond to network and security related incidents and provide continuous monitoring of our systems.
- BMC Helix has a variety of security tools implemented to protect its environment and data entrusted to it, including but not limited to, intrusion prevention services (IPS), anti-virus, application heuristic analysis (sandboxing), endpoint encryption, security information and event management (SIEM), rogue system detection (RSD), and web content filtering.
- BMC Helix maintains a formal incident response and cyber crisis plan that includes standard actions and engagement for incident handling that includes notification to the Customer and authorities.