Acceptable Use Policy for Contractors ("AUP")

Any person or entity as well as that person or entity's affiliate, subsidiary, employee, agent, supplier, subcontractor, processor, sub-processor or other representative of an entity (each a "**Representative**") (collectively the "**Contractor**") that provides products or services ("**Services**") to Stryker Corporation and/or any of Stryker Corporation's affiliates, subsidiaries, joint ventures of or including Stryker, its and their representatives, employees, directors, agents and other entities designated by Stryker (collectively and individually referred to as a "**Stryker** ") is bound by and must comply with the Stryker's AUP*.

In Accessing Stryker Systems or in connection with its provisioning of Services to Stryker pursuant to any agreement between Contractor and Stryker (the "**Agreement**"), Contractor agrees that the terms and conditions of this AUP are in addition to the terms and conditions specified in the Agreement and in the event of a conflict, the terms of this AUP shall control. Defined terms are as set for in Section 4 below. The term "including" means including without limitation. Whenever appropriate in this AUP, terms in the singular form shall include the plural (and vice versa) and any gender form shall include all others. The section headings in this AUP are for convenience and reference only and do not define, limit, or describe the scope or intent of any provisions of this AUP.

1. **Access to Stryker Data and Stryker Systems**. If Contractor is given Access to any Stryker Systems in connection with the Services, Contractor shall not tamper with, compromise, or circumvent any security or audit measures used in connection with the Stryker Systems. All Contractor connectivity to Stryker Systems and all attempts at the same shall only be through Stryker's security gateways/firewalls and only through Stryker-approved security procedures. Stryker may at its option require Contractor to use Stryker provided devices to make such connections. Contractor shall not Access, and shall not permit unauthorized persons or entities to Access, Stryker Systems and/or networks that contain Stryker Data without Stryker's express written authorization, and any such actual or attempted Access must be consistent with any such authorization.

2. **Security Controls.**

2.1 **Stryker Confidential Information**. All Stryker Data is, or shall be, and shall remain the property of Stryker and shall be deemed confidential information of Stryker, which Contractor must keep strictly confidential. Contractor shall not Access or attempt to Access, and shall not allow others to Access, Stryker Data or Stryker Systems to which it is not entitled or that is not required for the performance of the Services by Contractor. Contractor shall ensure that Access to Stryker Data or Stryker Systems shall be limited to those Representatives of Contractor that are authorized by Contractor and who are required to Access such Stryker Data and Access Stryker Systems solely to perform Contractor's obligations as set forth in the Agreement. Contractor shall comply and ensure Contractor's Representatives comply with all applicable laws and regulations in its performance of the AUP and the Agreement, including when Accessing Stryker Data and Stryker Systems. Contractor will ensure that Stryker shall have Access to and the ability to easily download any Stryker Data stored, hosted or controlled by Contractor or any of Contractor's Representatives at all times. Stryker shall have the right to remove, or require Contractor to remove, Stryker Data from the systems or software of Contractor or any of Contractor's Representatives. Contractor shall promptly comply (which shall in no event be longer than any time frame for compliance required by applicable laws and regulations) with any request from Stryker to Access, amend or erase any Stryker Data including as is necessary to allow Stryker to comply with applicable laws and regulations with respect to any Stryker Data involving Personal Data. Contractor shall assist Stryker in complying with its obligations of providing Access to Personal Data, deletion and/or rectification of Personal Data under any data protection or privacy laws and regulations and, if required by Stryker, return or delete all copies of Personal Data that are Accessed in accordance with the Agreement.

2.2 **Locations**. Contractor shall Access any and all Stryker Data and Stryker Systems only as permitted in the Agreement and solely in and from the country of origin unless authorized by Stryker in writing in advance (e.g., a statement of work executed by the parties identifying specific countries acceptable for Access).

2.3 **Restrictions on Use.** Notwithstanding anything in the Agreement to the contrary, Contractor shall not reverse engineer, combine, anonymize, de-identify, aggregate, or commingle any Stryker Data or use Stryker Data in a de-identified or aggregated form, or authorize, allow or enable any of its Representatives or other persons or entities to do the same and without Stryker's advance written approval (in its sole discretion). Stryker Data and Stryker Systems shall not be (a) used by Contractor other than solely as necessary for Contractor's performance of Contractor's obligations under the Agreement, (b) disclosed, sold, assigned, leased or otherwise provided to

unapproved third parties by Contractor, or (c) commercially exploited by or on behalf of Contractor. Contractor shall not possess or assert encumbrances or other rights in or to the Stryker Data and/or Stryker Systems.

2.4 **Disabling Devices**. Contractor shall take appropriate measures to ensure that Contractor systems connecting to Stryker Systems and Stryker Data do not contain any Disabling Device.

2.5 **Security Measures.** In addition to and without limiting Contractor's obligations under the Agreement, Contractor shall implement, monitor and maintain physical, operational, technical, administrative and organizational safeguards and other security measures that are no less rigorous than Industry Standards in its operations and the Services to (a) ensure the security and confidentiality of Stryker Data and Stryker Systems, (b) protect against any anticipated threats or hazards to the security or integrity of Stryker Data and Stryker Systems, (c) prevent a Security Incident, and (d) ensure the proper disposition of Stryker Data. Contractor shall not make any changes to its security measures that would adversely impact Stryker. Contractor shall comply with any additional requirements in relation to data protection or integrity that Stryker may from time to time reasonably request. Contractor shall be responsible and liable for the compliance with this AUP by, and the acts and omissions of, its Representatives. For the avoidance of doubt, the occurrence of a force majeure event shall not excuse or relieve Contractor of its obligations under this AUP. The foregoing security measures shall include multi-factor authentication and anti-hacking, data loss protection, encryption, and real-time intrusion detection. Contractor shall actively monitor the intrusion detection system for activities that correspond to attempts at breaking the security of the Services. Contractor shall adopt and follow operational procedures to disable the source of any perceived attack and escalation procedures to notify Stryker and Contractor security groups for follow-up action. If the Services involve the hosting of Stryker Data, all such data shall be hosted on servers located in a SOC 2 (applying the then-current standard) compliant hosting facility.

2.6 **Quality Control.** Contractor shall regularly audit, review, test and otherwise monitor its and its Representative's security measures to ensure their continued effectiveness and determine whether adjustments are necessary in light of circumstances including changes in law, regulation, technology, customer information systems or threats or hazards to Stryker Data and Stryker Systems. Contractor shall ensure that all its Representatives that Access any Stryker Data and Stryker Systems have been appropriately trained in the Security Controls. Contractor shall immediately inform Stryker, of any abnormalities and/or suspicious activity regarding the Services discovered by Contractor which may jeopardize or have compromised the security of Stryker Data and Stryker Systems or otherwise cause Contractor to violate the Agreement.

2.7 **Data Protection.** Contractor shall at all times encrypt Stryker Data at Industry Standard levels. In addition, Contractor shall ensure that all Stryker Data stored on shared media shall be at minimum logically partitioned (while at rest, in storage and in back up), easily extractable and not subject to a legal hold of any other client of Contractor.

2.8 **Multi Factor Authentication.** All Contractors Accessing Stryker Data or Stryker Systems shall supply, implement, and support a secure multi-factor method of authentication in accordance with NIST standards ("MFA"). At a minimum, the Contractor's MFA method shall include the requirement of two or more of the following different factors to achieve authentication: (i) a password or PIN; and (ii) a token. If utilizing APIs, the Contractor shall implement MFA verification into the API. The Contractor shall support a secure, multi-factor method of remote authentication and authorization to identified Contractor administrators that will allow Contractor designated personnel the ability to perform management duties on the system. If performing services on behalf of Stryker for GSA regulated entities, the Contractor shall support a secure, multi-factor method of remote authentication and authorization to identified Government administrators that will allow Government designated personnel the ability to perform management duties on the Contractor's system in accordance with GSA rules and regulations.

2.9 **Passwords.** Contractor shall implement and maintain a strict complex password policy for all Access to the Services, any Stryker Data and Stryker Systems that includes ensuring: (a) use of two factor authentication on equipment and software used to provide or within the Services; (b) that passwords are not re-used across devices or tools; (c) that user IDs and passwords are not delivered in the same unencrypted email message; (d) that passwords for user accounts have a minimum length of eight characters and are sufficiently complex; (e) that users requiring a password reset are not sent their actual password but are instead sent a complex, randomly generated password of at least eight characters, which the user would be forced to change at the next logon; (f) that passwords are changed whenever there is any indication of system or password compromise; and (g) that the passwords for resigned, terminated or reassigned Representatives of Contractor are properly changed or

the user account terminated (where appropriate) as soon as possible, but in no event more than 24 hours after resignation, termination or reassignment.

2.10 **Regulatory Documentation.** Upon Stryker's request as applicable, Contractor shall (and shall procure that any of its Representatives shall) execute any documentation required by Stryker to comply with the requirements under any applicable data protection and/or privacy laws and regulations (e.g., EU Commission approved Model Clauses, other documentation required to comply with the EU General Data Protection Regulation 2016/679, and Business Associate Agreement).

2.11 **Security Audit.** Contractor shall (at Stryker's request and at Contractor's cost) provide a report regarding security measures and controls. Such report shall be carried out by an independent third party appointed by Contractor, and the scope shall measure (through identification and testing of controls) compliance against the relevant criteria of the AUP, Agreement and Industry Standards. Upon notice to Contractor, Stryker may carry out or have carried out a security audit of the Services. Such Stryker audits shall occur no more than annually (except in the event of a Security Incident). Contractor shall make its Representatives available to the extent reasonably necessary to answer questions or otherwise assist Stryker in performing such audits and shall implement corrective action as may be identified by such audit. Upon Stryker's request, Contractor and its Representatives shall execute or cause to be executed any documentation required by Stryker to demonstrate compliance with its obligations under this AUP.

3. **Security Incidents**. If Contractor discovers or is notified of any Security Incident, then in each case Contractor shall:

3.1 within 24 hours of becoming aware thereof, notify Stryker of the date, facts and circumstances of such Security Incident, the nature and content of the Stryker Data and Stryker Systems so affected (including, with respect to Security Incidents involving Personal Data, the number of persons affected and, to the extent possible, the identities of the affected persons), and the steps Contractor has taken to investigate the Security Incident, mitigate potential harm and prevent further loss or theft, or further unauthorized, accidental or unlawful acquisition, destruction, loss, alteration, copying, disclosure, Access, use or processing of, the Stryker Data and Stryker Systems so affected;

3.2 be responsible for taking all actions necessary or recommended to remediate, mitigate and respond to such Security Incident, including (a) assembling and preserving pertinent information with respect to the Security Incident; (b) conducting a root-cause analysis to determine the cause(s) of the Security Incident, and providing Stryker with a detailed report indicating the cause(s) of the Security Incident and the plan to address and remediate the Security Incident; (c) documenting actions taken in response to the Security Incident in sufficient detail to meet reasonable expectations of forensic admissibility, and conducting a post-incident review of all events and actions taken, if any, with a view to making any needed modifications in business practices relating to the protection of Stryker Data and Stryker Systems; (d) minimizing the impact of and correcting any problems that contributed to the Security Incident; and (e) taking appropriate preventive measures so that such problems do not recur, including implementing new security measures to the extent required by any governmental authority or applicable laws and regulations, or otherwise appropriate;

3.3 as requested by Stryker, advise Stryker of the status of remedial efforts being undertaken with respect to the Security Incident;

3.4 cooperate with (a) any investigation relating to the Security Incident that is carried out at the direction of any governmental authority and (b) Stryker in all reasonable and lawful efforts to investigate, prevent the recurrence of, mitigate and rectify the Security Incident;

3.5 with respect to any Security Incident involving Personal Data, assist Stryker in providing notices (including as required by laws or regulations, including the PCI DSS) to any affected persons, governmental authorities or similar third parties, as determined by Stryker and if requested by Stryker. For the avoidance of doubt, the content of any filings, communications, notices, press releases or reports related to any Security Incident must be approved by Stryker prior to any publication or communication thereof; and

3.6 with respect to any Security Incident and notwithstanding anything to the contrary contained in the Agreement, pay for or reimburse Stryker for all costs and expenses incurred by Stryker in connection with investigating, addressing and responding to any such Security Incident, including (a) forensic and investigation

services to investigate the existence and cause of the Security Incident and the extent to which Personal Data was involved; (b) preparation and mailing or other transmission of notifications or other communications to any affected persons or governmental authorities or similar third parties as Stryker deems appropriate; (c) establishment of a call center or other communications procedures in response to the Security Incident; (d) credit monitoring, identity theft monitoring, fraud resolution and repair services for the affected persons; (e) public relations and other similar crisis management services; (f) legal, consulting and accounting expenses associated with Stryker's investigation of and response to the Security Incident; and (g) any governmental fines or penalties.

4. **Definitions**. The following terms shall have the following meanings as used in this AUP.

4.1 **"Access"** "**Accessing**" or "**Accessed"** means access, use, collect, obtain, maintain, handle, process, copy, record, organize, store, host, transmit, transfer, provide, disclose, make available, generate, change, dispose, erase or destroy.

4.2 "**Disabling Device**" means any programs, mechanisms, programming devices, malware or other computer code (a) designed to disrupt, disable, harm, or otherwise impede in any manner the operation of any software program or code, or any computer system or network (commonly referred to as "malware", "spyware", "viruses" or "worms"); (b) that would disable or impair the operation thereof or of any Stryker System or Stryker Data in any way based on the elapsing of a period of time or the advancement to a particular date or other numeral (referred to as "time bombs", "time locks", or "drop dead" devices); (c) is designed to or could reasonably be used to permit a party or any third party to access any Stryker System or Stryker Data (referred to as "trojans", "traps", "access codes" or "trap door" devices); or (d) is designed to or could reasonably be used to permit a party or any third party to track, monitor or otherwise report the operation and use of any Stryker System or Stryker Data.

4.3 "**Industry Standards**" means generally accepted industry standards for global firms providing the same or similar Services including (a) the Information Security Management Systems Requirements and ISO-IEC 27000 series; (b) the standards, practices and guidelines issued by the National Institute for Standards and Technology; (c) laws and other applicable industry standards; as each may be updated, amended or replaced"

4.4 "**Personal Data**" means data and/or information (a) alone or, when used in combination with other information, that identifies or is identifiable to an individual or (b) from which identification or contact information of an individual person can be derived. Personal Data can be in any media or format, including computerized or electronic records as well as paper-based files. Personal Data may include: (i) a first or last name or initials; (ii) a home or other physical address; (iii) an email address or other online contact information; (iv) a telephone number; (v) a social security number, tax ID number, driver's license number, passport number or other government-issued identifier; (vi) financial account numbers (including information that would permit Access to a financial account); (vii) birth dates; (viii) compensation, benefits, tax, marital/family status and other similar information; (ix) protected health information; (x) any other information by which one is reasonably able to personally identify a person; and (xi) any metadata related to the foregoing (i) through (x). Additionally, to the extent any other information (such as, case report form information, personal profile information, IP addresses, other unique identifiers, or biometric information) is associated or combined with Personal Data, then such information is also Personal Data.

4.5 "**Stryker Data**" means Personal Data and all other data and information (of any kind or nature whatsoever and in any form of media) provided by or on behalf of Stryker, generated, obtained, developed, processed or produced by, or obtained as a result of or in connection with the Services or the use of the Services (including any changes, improvement, enhancements or updates thereto) or otherwise Accessed by Contractor. Stryker Data includes but is not limited to all text, files, data, output, programs, files, information or material (a) of or submitted by or relating to Stryker or any of their representatives, users, customers or vendors, (b) residing on any Stryker Systems, or (c) generated, obtained, developed, processed or produced by, as a result of or in connection with the Services or the use of the Services by any Stryker or any of their representatives, users, customers or vendors, including any changes, improvement, enhancements or updates thereto.

4.6 **"Security Incident**" means any actual, threatened or suspected unauthorized, accidental or unlawful acquisition, destruction, loss, alteration, copying, disclosure, Access, use or processing of any Stryker Data or Stryker Systems.

4.7 **"Security Controls"** means the requirements of this AUP.

4.8 "**Stryker Systems**" means interfaces, databases, software, hardware, mobile applications, web sites or other systems (whether computer, electronic, digital or other technologies now or hereafter known) of any Stryker affiliates, contractors or customers.