Data Processing Addendum

1st February 2023, Version 2.1

SURGICAL XR PTY LTD, Suite 203, Level 2 Technology Place, Macquarie University, NSW 2109, Australian Business Number (ABN) of: 14 628 735 642
("Company," "we," "us',' "Surgical XR" or "our"), the Surgical XR Web Application (customer feedback platform), and www.Surgical XR.co (collectively referred as "Services") collects and processes Personal Data.

This Data Processing Addendum (the "DPA"), entered into by the Surgical XR Customer ("Customer") identified on the applicable Surgical XR ordering document ("Terms of Use") for Surgical XR Services and the Surgical XR company identified on the ordering document (along with its affiliates, "Surgical XR"), governs the processing of personal Data that Customer uploads or otherwise provides in connection with the Services.

This Addendum sets out the Data protection terms and conditions for the Customer's use of Surgical XR Services ("Services") and any other entity controlled by or under common control with Surgical XR. This DPA is supplemental to, and forms an integral part of, the Service Agreement and is effective upon its incorporation into the Agreement, which may be specified in the Agreement, an Order or an executed amendment to the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

HOW TO EXECUTE A SIGNED VERSION OF THIS DPA

Follow the link and review instructions:
1. This DPA consists of two parts: the main body of the DPA and Annexes 1,2, 3 and 4.
2. This DPA has been pre-signed on behalf of Surgical XR.
3. To complete this DPA, the Customer should complete the Data in the signature box and sign on Page 10.
4. Customers residing in European Economic Area or Switzerland also need to complete the Data in the signature box and sign on the Page 8 and the Page 10 of the Standard Contractual Clauses document SurgicalXR.com/sccs). This document forms Exhibit 3 of this DPA. It serves as a transfer mechanism for Data exports from EEA + Switzerland to the rest of the world, where Surgical XR has its operating units and sub processors.
5. Send the completed and signed DPA to Surgical XR by email. Upon receipt of the completed and signed DPA, Surgical XR will send you a confirmation email, and DPA will become legally binding.

1. Definitions
In addition to the capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth opposite each one of them:
"CCPA" means the California Consumer Privacy Act of 2018, together with any subordinate legislation or regulations.
"Controller-to-Processor SCCs" means the Standard Contractual Clauses (Processors) in the Annex 3 to the European Commission Decision of 4 June 2021, as may be amended or replaced from time to

time by the European Commission.
"Customer Personal Data" means Personal Data that Customer uploads or otherwise provides Surgical XR in connection with its use of Surgical XR's Services.
"General Data Protection Regulation" means Regulation (EU) 2016/679 of the European Parliament and the Council together with any subordinate legislation or regulation implementing the General Data Protection Regulation.
"Personal Data" means Data about an individual that:
● can be used to identify, contact, or locate a specific individual.
● can be combined with other data that can be used to identify, contact, or locate a specific individual.
● is defined as "Personal Data" or "personal Data" by applicable laws or regulations relating to the collection, use, storage, or disclosure of Data about an identifiable individual.
"Personal Data Breach" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.
"SCCs" means all Controller-to-Processor SCCs and Controller-to-Controller SCCs entered into between the parties under the Agreement.
"Subprocessor" means any entity which provides processing services to Surgical XR in furtherance of Surgical XR's processing of Customer Personal Data.
"Process" and its cognates mean any operation or set of operations which are performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"Supervisory Authority" means an independent public authority which is (i) established by a European Union member state according to Article 51 of the General Data Protection Regulation; or (ii) the public authority governing Data protection, which has supervisory authority and jurisdiction over Customer.

2. Customer's Processing of Personal Data
2.1 Within the scope of the Service Agreement and in its use of the Services, the Customer will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws concerning its Processing of Personal Data and the Instructions it issues to Surgical XR.
2.2 Customer acknowledges and agrees that they will be solely responsible for:
● The accuracy, quality, and legality of Customer Data and how they acquired Personal Data.
● Complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for collecting and using Personal Data, including obtaining any required consents and authorizations
● Ensuring you have the right to transfer or provide access to the Personal Data to us for processing under the terms of the Service Agreement (including this DPA).
● Ensuring that your Instructions regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws.
● Complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent, or managed through the Services, including those relating to obtaining consents (where required) to send emails, the content of the emails, and its email deployment practices.

3. Surgical XR's processing of Personal Data

3.1 Subject to the provisions of the Service Agreement, to the extent that Surgical XR's data processing activities are not adequately described in the Service Agreement, the Customer will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by Surgical XR.

Surgical XR will process the Personal Data only as outlined in the Customer's written instructions, and no Personal Data will be processed unless explicitly instructed by the Customer.

3.2 The Surgical XR will only process the Personal Data on documented instructions of the Customer to the extent that this is required for the provision of the Services. Should the Surgical XR reasonably believe that a specific processing activity beyond the scope of the Customer's instructions is necessary to comply with a legal obligation to which the Surgical XR is subject, the Surgical XR shall inform the Customer of that legal obligation and seek explicit authorization from the Customer before undertaking such processing.

The Surgical XR shall never process the Personal Data in a manner inconsistent with the Customer's documented instructions. The Surgical XR shall immediately notify the Customer if, in its opinion, any instruction infringes applicable data protection laws and regulations. Such notification will not constitute a general obligation on the part of Surgical XR to monitor or interpret the laws applicable to the Customer, and such notice will not constitute legal advice to the Customer.

3.3 The Parties have entered into a Service Agreement to benefit from the capabilities of Surgical XR in securing and processing the Personal Data for the purposes set out in Annex 2. The Data Processor shall be allowed to exercise its discretion in the selection and use of such means as it considers necessary to pursue those purposes, provided that all such intention is compatible with the requirements of this Data Processing Agreement, particularly the Customer's written instructions.

3.4 The Customer warrants that it has all necessary rights to provide the Personal Data to the Surgical XR for the processing to be performed concerning the Services and that one or more lawful bases outlined in EU Data Protection and other applicable privacy laws ("privacy laws") support the lawfulness of the processing. To the extent required by privacy laws , the Customer is responsible for ensuring that all necessary privacy notices are provided to data subjects, and unless another legal basis outlined in privacy laws supports the lawfulness of the processing, that any necessary data subject consents to the processing are obtained, and for ensuring that a record of such consents is maintained. Should such consent be revoked by a data subject, the Customer is responsible for communicating the fact of such revocation to the Surgical XR, and the Surgical XR remains accountable for implementing the Customer's instruction with respect to the processing of that Personal Data.

4. Confidentiality

4.1 Without prejudice to any existing contractual arrangements between the Parties, Surgical XR shall treat all Personal Data as confidential. It shall inform all its employees, agents, and/ or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data

4.2 Surgical XR shall take reasonable steps to ensure that access to the Customer Personal Data is limited on a need to know/access basis and that all Surgical XR's personnel receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access/use of Customer's Personal Data.

5. Security

5.1 Concerning the Customer Personal Data, Surgical XR shall implement appropriate technical and organizational measures to ensure a proper level of security, including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR. Surgical XR shall consider the risks presented by processing, particularly from a Personal Data Breach, when assessing the appropriate level of security.

5.2 A detailed list of security measures implemented by Surgical XR is located in Annex 2 of this document.

5.3 The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. Surgical XR will therefore evaluate the measures as implemented in accordance with Article 5 on an on-going basis in order to maintain compliance with the requirements set out in Article 5. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in EU Data Protection Law or any other applicable privacy law or by data protection authorities of competent jurisdiction.

5.4 Where an amendment to the Service Agreement is necessary in order to execute a Customer's instruction to Surgical XR to improve security measures, as may be required by changes in EU Data Protection Law or any other applicable privacy law, the Parties shall negotiate an amendment to the Service Agreement in good faith.

6. Sub Processing

6.1. Customer authorizes Surgical XR and each Surgical XR Affiliate to appoint (and permit each Sub Processor appointed under this Section 6) to select Sub Surgical XR in accordance with this Section 6 and any restrictions in the Addendum.

6.2. Surgical XR and each Surgical XR Affiliate may continue to use those Sub Processors already engaged by Surgical XR or any Surgical XR Affiliate as of the date of this DPA. The current list of Sub Processors used by Surgical XR and each Surgical XR Affiliate can be found here SurgicalXR.com/sub-processors

6.3. Surgical XR may appoint new Sub Processors and shall give notice of the appointment of any new Sub Processor (for instance, as part of a Privacy Policy update or Sub Processor list update), whether by general or specific reference to such Sub Processor (e.g., by name or type of Service), including relevant details of the processing to be undertaken by the new Sub Processor. If, within seven (7) days of such notice, Customer notifies Surgical XR in writing of any objections (on reasonable grounds) to the proposed appointment, Surgical XR shall not appoint for the processing of Customer Personal Data the proposed Sub Processor until reasonable steps have been taken to address the objections raised by Customer, and Customer has been provided with a reasonable written explanation of the actions taken.

6.4 Where such steps are not sufficient to relieve Customer's reasonable objections, then Customer or Surgical XR may, by written notice to the other Party, with immediate effect, terminate the Addendum to the extent that it relates to the Services which require the use of the proposed Sub Processor without bearing liability for such termination. Concerning each new Sub Processor, Surgical XR shall:

- Before the Sub Processor first Processes Customer Personal Data, take reasonable steps (for instance, by way of reviewing Privacy policy and Sub Processor list as appropriate) to ensure that the Sub Processor is committed to providing the level of protection for Customer Personal Data required by the Addendum; and
- Ensure that the arrangement between the Surgical XR and the Sub Processor is governed by a written contract, including terms that offer a materially similar level of protection for Customer Personal Data as those set out in this DPA that meet the requirements of applicable privacy laws.
- Ensure that the Surgical XR remains fully liable to the Customer for the Sub Processor's performance.

7. Data Subject Rights

7.1. Customer shall be solely responsible for compliance with any statutory obligations concerning requests to exercise Data Subject rights under Data Protection Laws (e.g., for access, rectification, deletion of Personal Data, etc.). Taking into account the nature of the Processing, Surgical XR shall reasonably endeavour to assist Customer insofar as feasible, to fulfil Customer's said obligations concerning such Data Subject requests, as applicable, at Customer's sole expense.

7.2. Surgical XR shall:

- Promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and
- Ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Surgical XR is subject, in which case Surgical XR shall, to the extent permitted by Applicable Laws, inform Customer of that legal requirement before it responds to the request.

8. Personal Data Breach

8.1 Surgical XR shall notify Customer without undue delay upon becoming aware of a Personal Data Breach affecting Customer Personal Data, in connection with the processing of such Customer Personal Data by the Surgical XR or Surgical XR's Affiliates. In such event, Surgical XR shall provide Customer with Data (to the extent in its possession) to assist Customer in meeting any obligations to inform Data Subjects or Data Protection authorities of the Personal Data Breach under the applicable privacy laws.

8.2 At the written request of the Customer, Surgical XR shall reasonably cooperate with the Customer and take such commercially reasonable steps as are agreed by the parties or necessary under applicable privacy laws to assist in the investigation, mitigation, and remediation of each such Personal Data Breach, at Customer's sole expense.

9. Data Protection Impact Assessment and Prior Consultation

9.1. At the written request of the Customer, Surgical XR and each Surgical XR's Affiliate shall provide reasonable assistance to Customer, at Customer's expense, with any Data protection impact assessments or prior consultations with Supervising Authorities or other competent Data privacy authorities, as required under any applicable Data Protection Laws. Such assistance shall be solely in relation to Processing of Customer Personal Data by Surgical XR.

10. Deletion or return of Customer Personal Data

10.1. Surgical XR shall promptly and in any event within up to sixty (60) days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "Cessation Date"), delete or pseudonymize all copies of those Customer Personal Data, except such copies as authorized including under this DPA or required to be retained in accordance with applicable law and/or regulation.

10.2. Subject to the Addendum, Surgical XR may retain Customer Personal Data to the extent authorized or required by Applicable Laws, provided that Surgical XR shall ensure the confidentiality of all such Customer Personal Data and shall ensure that it is only processed for such legal purpose(s).

10.3. Upon Customer's prior written request, Surgical XR shall provide written certification to Customer that it has complied with this Section 10.

11. Audit Rights

11.1. Subject to Sections 10.2 and 10.3, Surgical XR shall make available to a reputable auditor mandated by Customer in coordination with Surgical XR, upon prior written request, such Data necessary to reasonably demonstrate compliance with this DPA, and shall allow for audits, including inspections, by such reputable auditor mandated by the Customer concerning the Processing of the Customer Personal

Data by Surgical XR, provided that such third-party auditor shall be subject to confidentiality obligations.
11.2. Provisions of Data and audits are and shall be at Customer's sole expense and may only arise under Section 11.1 to the extent that the Addendum does not otherwise give Customer Data and audit rights meeting the relevant requirements of the applicable Data Protection Laws. In any event, all audits or inspections shall be subject to the terms of the Addendum and Surgical XR's obligations to third parties, including concerning confidentiality.
11.3. Customer shall give Surgical XR reasonable prior written notice of any audit or inspection to be conducted under Section 11.1. Customer shall use (and ensure that each of its mandated auditors uses) its best efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Surgical XR's business. Parties shall mutually agree upon the scope, timing, and duration of
the audit or inspection in addition to the reimbursement rate for which the Customer shall be responsible. Surgical XR need not give access to its premises for such an audit or review:
● To any individual unless they produce reasonable evidence of identity and authority;
● If Surgical XR was not given written notice of such audit or inspection at least two weeks in advance;
● Outside regular business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer has given notice that this is the case before attendance outside those hours begins; or
● For premises outside the Surgical XR's control (such as Data storage farms of AWS);
● For more than one (1) audit or inspection in any calendar year, except for any additional audits or inspections which:
i. Customer reasonably considers necessary because of genuine concerns as to Surgical XR's compliance with this DPA; or
ii. Customer is required to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where Customer has identified its concerns or the relevant requirement or request in its prior written notice to Surgical XR of the audit or inspection.
11.4 Customer shall reimburse Surgical XR for any time expended for any such on-site audit at the Surgical XR's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Surgical XR shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Surgical XR. The Customer shall promptly notify Surgical XR with Data regarding any non-compliance discovered during an audit, and Surgical XR shall use commercially reasonable efforts to address any confirmed non-compliance.

12. General Terms

12.1. Governing Law and Jurisdiction. This DPA is governed by the laws of the State of New South Wales, Australia. Any legal or equitable claim of any nature arising hereunder will be filed and maintained in the courts having jurisdiction in New South Wales, and the courts of appeal from them. The Parties to this DPA with this submit to the choice of jurisdiction stipulated in the Addendum concerning any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity. This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Addendum.
12.2. Order of Precedence. Nothing in this DPA reduces Surgical XR's obligations under the Addendum concerning the protection of Personal Data or permits Surgical XR to Process (or allow the Processing of)

Personal Data in a prohibited manner. In the event of any conflict or inconsistency between this DPA and the Privacy Policy (as defined under the Addendum), the Privacy Policy shall prevail provided only that the procedure prevailing through the Privacy Policy shall not constitute as a breach or infringement of any Applicable Laws. This DPA is not intended to, and does not in any way limit or derogate from Customer's obligations and liabilities towards the Processor under the Addendum, and/or according to the GDPR or any law applicable to Customer, in connection with the collection, handling and use of Personal Data by Customer or its Affiliates or other processors or their Sub Processors, including concerning the transfer or provision of Personal Data to Surgical XR and/or providing access thereto to Surgical XR.

12.3 In the event of inconsistencies between the provisions of this DPA and any other addendums between the Parties, including the Addendum and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) addendums entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

12.4 Changes in Data Protection Laws:

● Customer may by at least forty-five (45) calendar days prior written notice to Surgical XR, request in writing any variations to this DPA if they are required, as a result of any change in, or decision of a competent authority under any applicable Data Protection Law, to allow Processing of those Customer Personal Data to be made (or continue to be made) without breach of that Data Protection Law; and

● If Customer gives notice concerning its request to modify this DPA under Section 12.4:

i. Surgical XR shall make commercially reasonable efforts to accommodate such modification request; and

ii. Customer shall not unreasonably withhold or delay Addendum to any substantial variations to this DPA proposed by Processor to protect the Processor against additional risks or indemnify and compensate Processor for any further steps and associated costs with the variations made herein.

● If Customer gives notice under Section 12.4, the Parties shall promptly discuss the proposed variations and negotiate in good faith to agree and implement those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable. If the Parties are unable to reach such an addendum within 30 days, then Customer or Surgical XR may, by written notice to the other Party, with immediate effect, terminate the Addendum to the extent that it relates to the Services which are affected by the proposed variations (or lack thereof).

12.6 Law enforcement and surveillance requests. Surgical XR will review any governmental or regulatory body's binding order and challenge invalid law enforcement or surveillance requests. For valid requests, we will disclose only the minimum amount of Personal Data required by law and notify our customers to seek protection from disclosures. Please note that we will always inform our customers unless prohibited from doing so or if there is a clear indication of illegal conduct connected with the use of Surgical XR Services.

12.7. Severance. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

12.8 Data Transfers. For transfers of EU Personal Data to Surgical XR in a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing 'adequate' data protection, Surgical XR agrees it will use the form of the Controller-to-Processor SCCs available at SurgicalXR.com/sccs

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Addendum with effect from the later date set out below.

Customer: _____
Name: _____
Position: _____
Address: _____
Date: _____
Signature: _____

Processor: SURGICAL XR PTY LTD
Name: Terry Carney
Position: Founder - Director
Address: Suite 203, Level 2 Technology Place, Macquarie University, NSW 2109.
Date:
Signature:

Annex 1: Details of Processing of Customer Personal Data

This **Annex 1** includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data.

The Customer is user of Surgical XR web application and Surgical XR. Surgical XR may also automatically collect personal
data through cookies, beacons and other tracking technologies. The subject matter and duration of the Processing of the Customer Personal Data are set out in the Addendum, including the Privacy Policy as references therein and this DPA.

The nature and purpose of the Processing of Customer Personal Data.

Customer feedback, roadmap and announcements platform, as detailed in the Addendum and the Privacy Policy.

The types of Customer Personal Data to be processed are as follows:

- Contact details: first name and last name, business email address, image, workmates email addresses, business name, business subdomain, Social media profiles, mobile number, testimonials
- Financial Data: Data necessary for payment, including for invoicing purposes, such as billing details and credit card numbers.
- Written communications: notes, email and live chat sessions (request demo and contact fields), customer feedback, ideas and vote on ideas, comments, service enquiries
- Cookie data: as detailed in Privacy Policy
- Device data: device type, operating system, unique device identifiers, device settings, and geo-location data.
- Log data: (IP) address, browser type and version visited pages, the time and date of visit, the time spent on each page, and other details.

The categories of Data Subject to whom the Customer Personal Data relates to are as follows:

- Owners, employees, representatives or other individuals acting on behalf of party to which Surgical XR provides the Services.
- Other individuals with access to the "Dashboard" section within Surgical XR Service.
- Materials available by means of the App (Ideas, Roadmaps, Announcements) may constitute of texts, graphics, audio files, or computer software that contain Data about other Data subjects.

The obligations and rights of Customer:

The obligations and rights of Customer and Surgical XR Affiliates are set out in the Addendum and this DPA.

Annex 2: Security measures

For purposes of keeping Customer and end-user Data ("Customer Data") safe and secure, Surgical XR is committed to complying with industry-standard privacy and security measures, as well as with all applicable Data privacy and security laws and regulations. This includes ensuring that Surgical XR's systems and infrastructure are protected against unauthorized or accidental access, loss, alteration, disclosure, or destruction. Surgical XR has taken all necessary technical and operational measures to organize and protect its facilities, hardware, and software, personnel, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, and incident response measures.

Preventing Unauthorized Product/Infrastructure Access. Surgical XRs system installation uses a hardened, patched OS with dedicated firewall and VPN services that help block unauthorized access. We also employ industry-leading solutions to mitigate DDoS attacks. The application is continually updated on weekly basis with the most recent and secure solutions. Critical security patches are provided as needed outside of the regular release cycle and specifically announced with email notifications and via our Twitter channel.

Authentication. User passwords are one-way salted and hashed before being stored. There is no way to recover and/or otherwise reverse-engineer passwords.

Employee access. A limited number of our trained employees have access to the products and to customer Data via controlled interfaces. The purpose of enabling employee access is to provide efficient customer support, detect and respond to security incidents, troubleshoot potential problems, and facilitate Data security. Employees are granted access by role, and all such access requests are logged.

Physical and environmental security. The application and user data are hosted by Amazon Web Services servers. You can see how AWS secures data here. Amazon's GDPR commitment is available here. AWSs physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications - details of AWS compliance can be found here. Surgical XR PTY LTD has not undergone any of the following audits: SOC Type 1/2, ISO, PCI DSS or FedRAMP

Third-party processing. In order for us to provide our customers with the Service in accordance with our DPA, we maintain contractual relationships with vendors. This includes contractual addendums, privacy policies, and vendor compliance programs. All our vendors are vetted for privacy and security compliance during and after their engagement with us.

Network security. Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The implemented technical measures differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules. We have implemented a Web Application Firewall (WAF) solution to protect internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Penetration testing. Our servers are under constant surveillance by AWS Guard Duty and Beagle Security with security audits performed every quarter in accordance with AWS Security Audit Guidelines.

Bug bounty. We currently do not support a bug bounty program, however you can report all issues to mailto:security@SurgicalXR.comand issues will be judged on a case by case basis. All reported issues and security holes are fixed with the highest priority.

Data is encrypted while in transfer & at rest. All private data to and from Surgical XR is transmitted over SSL. Data stored within the Surgical XR infrastructure is encrypted at rest

Event logging. Surgical XR systems employ a number of mechanisms to log and trace events that happen within the system. Theses cover user actions, security events and system alarms

Credit Card Information. All credit card information is stored within Stripe. Once you submit your credit card information on the forms, that information is sent directly from your web browser to Stripe via HTTPS, it doesn't ever touch Surgical XR servers. Credit card information is never stored within the Surgical XR infrastructure.

The only information viewable is:

- Credit card type (Visa, Mastercard, etc.)
- Last 4 digits of the card number
- Expiration date

Only the company founders have access to the Stripe accounts.

Infrastructure availability. The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime.
Business Continuity. Surgical XR shall maintain policies and procedures to ensure that Surgical XR may continue to perform business-critical functions in the face of an extraordinary event. This includes Data center resiliency and disaster recovery procedures for business-critical Data and processing functions.
Annex 3: Standard Contractual Clauses
If you reside in the European Economic Area or Switzerland, please download pre-signed Surgical XR Standard Contractual Clauses (Controller to Processor) found on the following link: SurgicalXR.com/sccs
Annex 4: Subprocessors
The controller has authorized the use of the following sub-processors: SurgicalXR.com/sub-processors

Suite 203, Level 2 Technology Pl,
Macquarie University NSW 2109
W: www.surgicalxr.com
E: contact@surgicalxr.com