AGREEMENT #: W911QY-20-C-0119 FLOWDOWN REQUIREMENTS FOR SUBCONTRACTS

(Appendix A) Dated 3-9-2022

This appendix applies to any subcontracts in support to AstraZeneca prime agreement with US Government W911QY-20-C-0119

Note: This Appendix A, dated 3-9-2022, incorporates the following FAR and DFAR clauses related to government property: 52.245-1, 52.245-9, 252.245-7001, 252.245-7002, 252.245-7003, 252.245-7004, and 252.211-7007.

In Appendix A, "Subcontractor" means the "Supplier" , "Subcontract" means this "Agreement.", "Subawardee" means any contractor that has been contracted by Subcontractor to provide goods and services in support of this Agreement.

Subcontractor understands and acknowledges that AstraZeneca is performing Contract No. W911QY-20-C-0119 for the United States Government.

GOVERNMENT SUBCONTRACT

As a prime contractor to US Government, AstraZeneca must comply with specific provisions of the Contract, including ensuring that any subcontractors supporting AstraZeneca comply with the terms in the Contract that flow down to subcontractors.

The work required under this Agreement will be performed in support of AstraZeneca's Contract with Government. As a Subcontractor under the Contract, Subcontractor must meet certain AstraZeneca's requirements under its prime agreement with Government. Subcontractor confirms that it is eligible to perform subcontracting work under a government contract and agrees with the Terms & Conditions/Flowdowns listed in this Appendix. Further, to the extent the Subcontractor must enter into subawards to fulfil requirements of this Agreement or any service hereunder W911QY-20-C-0119 Subcontractor shall take full responsibility to ensure that its subawardees are in full compliance with all applicable Federal procurement laws and regulations and pertinent subcontract requirements, as set in this Appendix.

Subcontractor acknowledges and understands that the Government is a third-party beneficiary to this Agreement and is entitled to the rights and benefits hereunder and may enforce the provisions hereof as if it were a party hereto.

Communication/notification required under this Agreement from/to the Subcontractor to/from Government shall be made through AstraZeneca.

Should any of the terms and conditions contained in Appendix A contradict those elsewhere in the Agreement, or any Statement of Work under the Agreement, then the terms and conditions of Appendix A shall supersede all others.

1. CONFIDENTIAL INFORMATION

"**Confidential information**", as used in this article, means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.

AstraZeneca and the Subcontractor may, by mutual consent, identify elsewhere in this Agreement specific information and/or categories of information which the AstraZeneca will furnish to the Subcontractor or that the Subcontractor is expected to generate which is confidential. Similarly, AstraZeneca and the Subcontractor may, by mutual consent, identify such confidential information from time to time during the performance of the contract. Failure to agree will be settled pursuant to the "Disputes" clause.

If it is established elsewhere in this Agreement that information to be utilized under this Agreement, or a portion thereof, is subject to the Privacy Act, the Subcontractor will follow the rules and procedures of disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.

Confidential information, as defined in paragraph (a) of this article, shall not be disclosed without the prior written consent

of the individual, institution, or organization.

Whenever the Subcontractor is uncertain with regard to the proper handling of material under the Agreement, or if the

material in question is subject to the Privacy Act or is confidential information subject to the provisions of this article, the Subcontractor shall obtain a written determination from AstraZeneca prior to any release, disclosure, dissemination, or publication.

AstraZeneca Determinations will reflect the result of internal coordination with appropriate program and legal officials.

The provisions of this Article shall not apply to conflicting or overlapping provisions in other Federal, State or local laws.

Subcontractor shall include the requirements set forth in this Article in all Sub-awards entered into after the date of effectiveness of this Agreement. Subcontractor acknowledges that confidential information will not be provided to sub-agreement holders unless or until Article 1 flows down to the relevant sub-agreement, and such entity agrees to be in substantial compliance with this Article.

Subcontractor further understands and agrees that AstraZeneca may provide Confidential Information in regard to this Agreement (including information exchanged pursuant to an existing confidentiality or nondisclosure agreement) to representatives or agents of the U.S. Government in connection with AstraZeneca's prime Contract W911QY-20-C-0119. AstraZeneca takes commercially reasonable steps to restrict their disclosure by the U.S. Government under applicable public disclosure / transparency laws. AstraZeneca, however, shall have no liability for the U.S. Government's release of any Subcontractor Confidential Information.

2. QUARTERLY MEETINGS

Subcontractor may need to participate in project meetings with Government and AstraZeneca. These meetings may be either teleconference or include face-to-face meetings with US Government in Washington, D.C , AstraZeneca or Subcontractor location, and at work sites of the Subcontractor. Such meetings may include, but are not limited to, meetings with the Subcontractor to discuss study designs, site visits to the Subcontractor's facilities, and meetings with AstraZeneca and Government officials to discuss agreement progress in relation to the Agreement deliverables, as well as study designs, technical, regulatory and ethical aspects of the program.

3. INSPECTION/ACCEPTANCE

A. Inspection: Subcontractor agrees that AstraZeneca and Government have the right to inspect and test all work called for by this Agreement, to the extent practicable at all places and times, including the period of performance, and in any event before acceptance. AstraZeneca and the Government may also inspect the premises of the Subcontractor or any of itsSub-awardees engaged after the Effective Date, with seven (7) days advance notice to the Subcontractor or any such Sub-awardee. The scope and duration of any such inspection will be mutually agreed between the Parties in writing in advance, such agreement not to be unreasonably withheld. AstraZeneca and the Government shall perform inspections and tests in a manner that will not unduly delay the work and will be subject to the Subcontractor's or its subawardees', as applicable, policies and procedures regarding security and facility access at all times while on the premises. If AstraZeneca and the Government perform any inspection or test on the premises of the Subcontractor or its Sub-awardee, the Subcontractor shall furnish, and shall require subawardees to furnish, at no increase in price, all reasonable facilities and assistance for the safe and convenient performance of these duties. Except as otherwise provided in the Agreement, AstraZeneca and/or the Government shall bear the expense of such inspections or tests made at other than the Subcontractor's or its Sub-awardee's premises.

B. Acceptance: Subcontractor agrees that AstraZeneca and/or Government shall inspect/accept or reject the work as promptly as practicable after completion/delivery, unless otherwise specified in the Agreement. AstraZeneca and/or Government failure to inspect and accept or reject the work shall not relieve the Subcontractor from responsibility, nor impose liability on AstraZeneca for nonconforming work. Work is nonconforming when it is defective in material or workmanship or is otherwise not in conformity with Agreement requirements. AstraZeneca and/or Government have the right to reject nonconforming work. Inspection/Acceptance of the supply deliverables should not exceed 90 days after completion.

4. FDA INSPECTIONS

In the event of an FDA inspection that occurs in relation to this contract and for the product, or for any other FDA inspection

that has the reasonable potential to impact the performance of this contract, the Subcontractor shall provide AstraZeneca with an exact copy (non-redacted) of the FDA Form 483 and the Establishment Inspection Report (EIR). The Subcontractor shall provide AstraZeneca with the copies of the plan for addressing areas of non-conformance to FDA regulations for GLP, GMP, or GCP guidelines as identified in the audit report, status updates during the plans execution and a copy of all final responses to the FDA. The Subcontractor shall also provide copies of any FDA audits received from its subawardees that occur as a result of this contract or for this product. The Subcontractor shall make arrangements for AstraZeneca and/or Government (s) to be present during the final debrief by the regulatory inspector.

Subcontractor shall notify AstraZeneca within 5 business days of a scheduled FDA audit or within 24 hours of an ad hoc site visit/audit if the FDA does not provide advanced notice.

Subcontractor shall provide copies of any FDA audit report that occur as a result of this contract or for this product within 1 business day of receiving correspondence from the FDA or third party.

Within 5 business days of audit report, Subcontractor shall provide AstraZeneca with a plan for addressing areas of nonconformance, if any are identified

5. COMPTROLLER GENERAL ACCESS TO RECORDS:

To the extent that the total Government payment under this Subcontract exceeds $5,000,000, the Comptroller General, at its discretion, shall have access to and the right to examine records relating to performance under this Agreement of any entity that participates in the performance of this Agreement for a period of three years after final payment is made.

This paragraph only applies to any record that is created or maintained in the ordinary course of business or pursuant to a provision of law. The terms of this paragraph shall be included in all lower tier sub-agreements to the Agreement.

The Comptroller General may not examine records pursuant to a clause included in an agreement more than three years after the final payment is made by the United States under the agreement.

6. FINANCIAL MATTERS

Subcontractor shall maintain adequate records to account for all costs incurred under this Agreement for which Subcontractor seeks reimbursement. Neither the Cost Accounting Standards nor any other aspect of the Federal Acquisition Regulation or its supplements apply to Subcontractor's accounting of costs under this Agreement.

Cost shall be accounted for in accordance with Subcontractor's commercial accounting system and practices which comply with International Financial Reporting Standards and the requirements of this Agreement, in which all costs, cash receipts and disbursements under this Agreement are controlled and documented properly.

7. QA AUDITS

AstraZeneca and Government reserves the right to participate in QA audits performed by the Subcontractor. Upon completion of the audit/site visit to its Sub-awardees, the Subcontractor shall provide a report capturing the findings, results and next steps in proceeding with the sub-awardee. If action is requested of the sub-awardee, detailed concerns for addressing areas of non-conformance to FDA regulations for GLP, GMP, or GCP guidelines, as identified in the audit report, must be provided to AstraZeneca. The Subcontractor shall provide responses from the sub awardees to address these concerns and plans for corrective action

The Subcontractor shall notify AstraZeneca a minimum of 15 business days in advance of upcoming, audits/site visits of its sub-awardees.

The Subcontractor shall notify AstraZeneca within 10 days of report completion.

AstraZeneca will review the report and provide a response to the Subcontractor within 15 business days

8. INCIDENT REPORT

Subcontractor shall communicate to AstraZeneca and document all critical programmatic concerns, issues, or probable risks that have or are likely to significantly impact project schedule and/or cost and/or performance. "Significant" is frequently defined as a 10% or greater cost or schedule variance within a control account, but should be confirmed in consultation with the AstraZeneca. Incidents that p3resent liability to the project even without cost/schedule impact, such as breach of GCP during a clinical study, must also be reported.

Incidents to be reported within the below timeframes:

- Due within 24 hours of activity or incident or within 12 hours for a security activity or incident
- Email or telephone with written follow-up to AstraZeneca
- Additional updates due to AstraZeneca within 24 hours of additional developments
- Subcontractor shall submit within 3 business days a Corrective Action Plan (if deemed necessary by either party) to address any potential issues
- If corrective action is deemed necessary, Subcontractor must address in writing, its consideration of concerns raised by AstraZeneca or Government within 3 business days of receiving such concerns

9. SCIENTIFIC PUBLICATIONS AND PRESS RELEASES

A. The Subcontractor shall not publish, release any reports, manuscripts, press releases, or abstracts about the work being performed under this Agreement without written concurrence with AstraZeneca.
B. Unless authorized in writing by AstraZeneca and Government, the Subcontractor shall not display Government logos including Operating Division or Staff Division logos on any publications.
C. The Subcontractor shall not reference the products(s) or services(s) awarded under this contract in commercial advertising, as defined in FAR 31.205-1, in any manner which states or implies Government approval or endorsement of the product(s) or service(s) provided.
D. The Subcontractor shall include this Article, including this clause and section (c) in all subawards where the Sub-awardee may propose publishing the results of its work under the subaward. The Subcontractor shall acknowledge the support of the Government whenever publicizing the work under this Agreement in any media by including an acknowledgement substantially as follows:

"This project has been funded in whole or in part by the U.S. Government under Agreement No. W911QY-20-C-0119. The US Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon."

10. REGULATORY COMPLIANCE.

A. Subcontractor agrees that if the scope of this Agreement includes any manufacturing, the Subcontractor will comply with Current Good Manufacturing Practices (cGMP) regulations at 21 CFR 210 and 211. Production shall occur using cGMP validated manufacturing process, fully compliant with 21 CFR 210 and 211, for bulk drug substance and fill and finished drug product, with a ramp-up capacity that provides doses sufficient for the government to treat the US population.
B. Production and distribution shall comply with applicable provisions of the Drug Supply Chain Security Act (DSCSA), Sections 581-585 of PL 113-54 (Nov 27, 2013), taking into account FDA's regular guidance for the COVID-19 public health response.
C. The clinical trial will comply with ICH Good Clinical Practices (GCP) regulations at 21 CFR Part 11.

11. QUALITY AGREEMENT

A. The Subcontractor agrees to have a Quality Agreement, acceptable by AZ, in place within 30 days of the execution of this Agreement, in conformance to AstraZeneca Quality Agreement (Insert as an Appendix once Government approves AZ Quality Agreement).

B. The Subcontractor will ensure appropriate quality agreements are in place with applicable subawardees to enable the Subcontractor to comply with its quality obligations to AstraZeneca , in accordance with FDA guidance and regulations, including but not limited to the November 2016 Guidance for Industry, "Contract Manufacturing Arrangements for Drugs: Quality Agreements, aligned with AstraZeneca Quality Agreement in Appendix C.

12. FOREIGN ACCESS TO DATA.

Export Compliance. The Parties will comply with any applicable U.S. export control statutes or regulations in performing this Agreement.

13. DISCLOSURE OF INFORMATION.

A. Performance under this Agreement may require the Subcontractor to access non-public data and information proprietary to a Government agency, another Government contractor, or of such nature that its dissemination or use other than as specified in the work statement would be adverse to the interests of the Government or others. Neither the Subcontractor, nor Subcontractor personnel, shall divulge nor release data nor information developed or obtained from or on behalf of the AstraZeneca or Government under performance of this Agreement which information specifically relates to AZD7442 (*i.e.*, would not apply more broadly to AstraZeneca's or Subcontractor's other antibody programs, such as its manufacturing platform), except as authorized by Government personnel or upon written approval of the AstraZeneca in accordance with OWS or other Government policies and/or guidance. The Subcontractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as specified in this Agreement, or any information at all regarding this agency.

B. The Subcontractor shall comply with all Government requirements for protection of non-public information. Unauthorized disclosure of nonpublic information is prohibited by the Government's rules. Unauthorized disclosure may result in termination of the Agreement, replacement of an Subcontractor employee, or other appropriate redress. Neither the Subcontractor nor the Subcontractor's employees shall disclose or cause to be disseminated, any information concerning the operations of the activity, which could result in, or increase the likelihood of, the possibility of a breach of the activity's security or interrupt the continuity of its operations.

C. No information related to data obtained under this Agreement shall be released or publicized without the prior written consent of the AstraZeneca.

14. FINANCIAL DISCLOSURE BY CLINICAL INVESTIGATORS

The Subcontractor does and shall comply with the requirements of 21 CFR Part 54, Financial Disclosure by Clinical Investigators.

15. ORGANIZATIONAL CONFLICTS OF INTEREST

Performance under this contract may create an actual or potential organizational conflict of interest such as are contemplated by FAR Part 9.505-General Rules. The contractor shall not engage in any other contractual or other activities which could create an organizational conflict of interest (OCI).

This provision shall apply to the prime contractor and all sub-Contractors. This provision shall have effect throughout the period of performance of this contract, any extensions thereto by change order or supplemental agreement, and for two (2) years thereafter. The government may pursue such remedies as may be permitted by law or this contract, upon determination that an OCI has occurred.

The work performed under this contract may create a significant potential for certain conflicts of interest, as set forth in FAR Parts 9.505-1, 9.505-2, 9.505-3, and 9.505-4. It is the intention of the parties hereto to prevent both the potential for bias in connection with the Contractor's performance of this contract, as well as the creation of any unfair competitive advantage as a result of knowledge gained through access to any non-public data or third party proprietary information.

The contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI. Furthermore, the contractor shall promptly submit a plan to the

Contracting Officer to either avoid or mitigate any such OCI. The Contracting Officer will have sole discretion in accepting the Contractor's mitigation plan. In the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, other remedies may be taken to prohibit the contractor from participating in contract requirements related to OCI.

Whenever performance of this contract provides access to another Contractor's proprietary information, the Contractor shall enter into a written agreement with the other entities involved, as appropriate, in order to protect such proprietary information from unauthorized use or disclosure for as long as it remains proprietary; and refrain from using such proprietary information other than as agreed to, for example to provide assistance during technical evaluation of other Contractors' offers or products under this contract. An executed copy of all proprietary information agreements by individual personnel or on a corporate basis shall be furnished to the CO within fifteen (15) calendar days of execution.

16. FEDERAL ACQUISITION REGULATION (FAR) AND DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS) CLAUSES INCORPORATED BY REFERENCE

The Federal Acquisition Regulation (FAR) and the Department of Defense FAR Supplement (DFAR) clauses incorporated herein shall have the same force in effect as if printed in full text. Full text can be found on http://www.acquisition.gov. Wherever necessary to make the context of the clauses set forth below applicable to this Subcontract Agreement, the term "Contractor" shall mean "Subcontractor," the term "subcontractor" shall mean "lower-tier subcontractor," the term "Contract" shall mean this Subcontract Agreement, the term "subcontract" shall mean "lower-tier subcontract," and where noted or necessary to derive proper meaning, the term "Government" and "Contracting Officer" do not change:

1. In the Phrases "Government Property," "Government Furnished Property" and "Government Owned Property."

2. In the patent clauses incorporated herein.

3. When a right, act, authorization, or obligation can be granted or performed only by the Government's duly authorized representative.

4. When title to property is to be transferred directly to the Government.

5. When access to proprietary financial information or other proprietary data is required except for authorized audit rights.

6. Where specifically modified herein.

Except as otherwise provided in this subcontract, the term "Subcontract" includes, but is not limited to, purchase orders and changes and modifications to purchase orders under this Subcontract.

FAR Clauses

52.203-6 Restrictions on Subcontractor Sales to the Government (Jun 2020) with Alternate I (Oct 1995)

52.203-13 Contractor Code of Business Ethics and Conduct (June 2020) (41 U.S.C. 3509).

52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)

52.204-10 Reporting Executive Compensation and First Tier Subcontract Awards (Jun 2020)

52.204-21 Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)

52.204-23 Prohibition on Contracting for Hardware, Software and Services Developed or Provided by Kapersky Lab and Other Covered Entities (July 2018)

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020)

52.209-6 Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended or Proposed for Debarment (Jan 2020)

52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)

52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tiersubcontracts that offer subcontracting opportunities.

52.219-9 Small Business Subcontracting Plan (Jun 2020) (15 U.S.C. 637(d)(4)).

52.222-21 Prohibition of Segregated Facilities (April 2015)

52.222-26 Equal Opportunity (Sept 2016)

52.222-35 Equal Opportunity for Veterans (Jun 2020)

52.222-36 Equal Opportunity for Workers with Disabilities (Jun 2020)

52.222-37, Employment Reports on Veterans (Jun 2020)

52.222-40 Notification of Employee Rights Under National Labor Relations Act (Dec 2010)

52.222-41, Service Contract Labor Standards (Aug 2018)

52.222-50 Combatting Trafficking in Persons (Jan 2019)

52.223-18 Encouraging Contractor Policies to Ban Text Messaging While Driving (Jun 2020)

52.225-13 Restrictions on Certain Foreign Purchases (Jun 2008)

52.232-40 Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)

52.233-3 Protest After Award (Aug 1996)

52.233-4 Applicable Law for Breach of Contract Claim (Oct 2004)

52.245-1 Government Property

52.245-9 Use and Charges

<u>DFARS Clauses</u>

252.203-7002 Requirement to Inform Employees of Whistleblower Rights (Sept 2013)

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)

252.209-7004 Subcontracting with Firms that are Owned or Controlled by the Government of a Terrorist Country (May 2019)

252.211-7003 Unique Item Identification and Valuation (Mar. 2016)

252.225-7048 Export Controlled Items (Jun 2013)

252.244-7000 Subcontracts for Commercial Items (Oct 2020)

252.245-7001 Tagging, Labeling, and Marking of Government-Furnished Property

252.245-7002 Reporting Loss of Government Property

252.245-7003 Contractor Property Management System Administration

252.245-7004 Reporting, Reutilization, and Disposal

252.211-7007 Reporting of Government-Furnished Property

(1) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(2) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(c) Exceptions. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract or agreement performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Agreements Officer, unless elsewhere in this contract or agreement are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil.

2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts, sub-agreements and other contractual instruments, including subcontracts for the acquisition of commercial items.

16. HEALTH RESOURCES PRIORITIES AND RATING SYSTEM (HRPAS) PRIORITY RATING

Not applicable

17. SECURITY PLAN

(1) The Subcontractor agrees to implement security plans aligned to the standards outlined in Section 18 (2) (provided upon AstraZeneca AZD7442 Project Security Standard). It is a requirement for the subcontractor to ensure appropriate steps are taken to achieve the objective of each security measure.

Subcontractor shall also use commercially reasonable efforts to ensure all its sub-awardees, consultants, researchers, etc. performing work on behalf of this effort, comply with Security requirements outlined in Section 18 (2).

I.

However, the AstraZeneca acknowledges that, in order to combat the global pandemic and launch AZD7442 as quickly as possible, the Suppler has entered into a number of contracts prior to the Execution Date. The Subcontractor will flow-down the provisions of the Project Security Standard to (i) all sub-agreements/contracts executed after the Execution Date, and (ii) all sub-agreements/contracts executed prior to the Execution Date which cover manufacturing/fill/finish/storage activities under this Agreement; provided that in no event will the Subcontractor be required to flow-down any provisions to any sub-Subcontractor which has a pre-existing direct relationship with the Government. The Subcontractor will have a period of ninety (90) days to amend any existing agreements to reflect these flow-down requirements or, in the alternative, to demonstrate the sub-Subcontractor's material compliance with any such flow-down requirements.

(2) AstraZeneca AZD7442 Project Security Standard

AstraZeneca
Global Security

AstraZeneca AZD7442 Project Security Standard

Global consolidated security standards for the Covid-19 vaccination and monoclonal antibody program.

Issue 1.01

Table of Contents

1 Purpose and scope

This document sets out the facility and supply chain security standards required of all parties involved in the AstraZeneca Novel Coronavirus AZD1222 and AZD7442 vaccine (the vaccine).

These standards are to be implemented by all organisations involved in the vaccine development, manufacture, packaging, transport & distribution and related activities.

These standards provide direction on security risk mitigation measures across all aspects of physical and procedural security.

Organisations may adapt security measures as needed to fit the nature and scale of the sites and resources committed to the vaccine project. It is a requirement for all organisations[1] to ensure appropriate steps are taken to achieve the objective of each security measure.

Advice from security and subject matter experts, can be obtained by contacting AstraZeneca Global Security GlobalSecurity@astrazeneca.com.

Insider threat and cyber security requirements are listed at section 10 below and provided separately by AstraZeneca Cyber Security Governance SecurityGovernance@astrazeneca.com

1.1 Review & assurance

Each organisation is responsible for preparing a Project Security Plan (PSP) to record compliance with this standard. PSPs do not have to follow the structure of this standard nor be a single document but may be a collection of documents e.g. Site Security Plan (SSP), Crisis Management Plan (CMP), IT and Cyber Security Plan etc.

PSPs must set out how each measure below is being implemented with sufficient evidence to enable independent validation.

If measures cannot be met immediately, remediation steps must be set out together with an implementation timeframe and communicated to AstraZeneca.

Plans and or remediation strategies must be submitted to AstraZeneca within 25 days of receipt of this document.

AstraZeneca (or its appointed agent) is entitled to visit all areas covered by this PSP to audit any organisation's compliance with its submitted PSP(s).

[1] Including all commercial outsoursed manufacturers, logistics providers, warehouses and subcontractors that produce, process or transport AZD7442 and AZD1222 drug substance, drug product and related packaging and labelling material.

2 Governance

All PSPs prepared in the implementation of this standard must include a description of governance structure responsible for ensuring compliance, specifically including:

2.1 Strategic oversight

Each organisation must identify the executive body/individual(s) responsible for ensuring implementation and compliance with this standard. This should include the means by which oversight is conducted.

2.2 Operational security management

Each organisation must identify the operational manager/individual(s) responsible for implementation and enforcement of the PSP. Operational managers must escalate non-adherence and breaches of security measures.

All plans must clearly identify the individual(s) responsible for security at each management level.

Organisations should nominate a single point of contact to handle security incidents and to support AstraZeneca investigation and introduce this person to AstraZeneca Global Security.

3 Threat and risk assessment

Each organisation must implement a security risk assessment program in accordance with ISO 31000:2009 Risk Management Principles and Guidelines.

ISO 31000:2009 comprises of the following activities:

- Communication and consultation.
- Establishing the context.
- Risk assessment.
  - Risk identification.
  - Risk analysis.
  - Risk evaluation.
- Risk treatment.
- Monitoring and review.

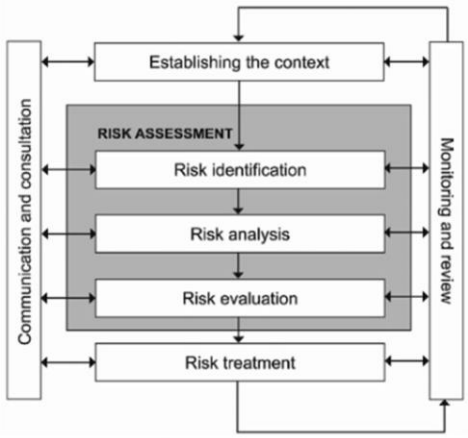

Figure 1 ISO 31000:2009

The risk assessment should be programmatic and cover the entire vaccine program including sites, transportation, communications and all related activities. Organisations should consider the need for sub-risk assessments for individual component parts of the program, for example site risk assessments.

3.1 AZD7442 identified threats

The following threats must be considered when identifying security risks:

- Theft / losses / missing item(s), including any drug product / drug substance / packed product or packaging components and any waste.
- Counterfeiting.
- Product diversion.
- Supply chain fraud and corruption.
- Disinformation activity.
- Direct action and disruptive protest activity.
- Product tampering, contamination/sabotage and extortion.

4 Crisis and incident response

It is anticipated that crisis management processes will be set out in a separate Crisis Management Plan (CMP), these may be attached to the PSP as an appendix. This security standard provides the minimum requirement for crisis management in relation to the vaccine program.

Each organisation must have in place:

- An identified crisis management structure consisting of at least one dedicated crisis management team.
- A crisis management plan (CMP).
- A training and exercising program (a minimum of one session to be devoted to a vaccine programme-related response).

Every site should have site specific incident response plans and response capability aligned to the risk profile of the site. Site plans should be reviewed and updated with vaccine program specific risks considered.

5 Security incident reporting

Organisations must notify AstraZeneca of any security incident in a timely manner. A security incident is any instance of crime or disruptive activity that threatens the safety of the vaccine program's people, assets, operation and reputation.

It specifically includes but is not limited to:

- Loss, theft or tampering of any vaccine related products, processes and information.
- Counterfeiting related activity.
- Fraud, product diversion/substitution or misrepresentation of the vaccine project.
- Actual or suspected disruptive (e.g. protest, threats, extortion etc) activity directed at the program.

Reporting should be as prompt as possible and always within 1 working day.

A principle of prudent, internal, overreaction (PIA) should be applied. Incidents should be assessed on a credible worst-case basis and organisations should default to prompt escalation and notification of incidents.

5.1 Notification

Organisations should notify their AstraZeneca relationship manager and copy all correspondence, in English, to globalsecurity@astrazeneca.com. Organisations should escalate and use other contact points as they deem reasonable given the severity and/or sensitivity of the report.

5.1.1 Evidential recording and investigation

Organisations should nominate a single point of contact to handle security incidents and to support AstraZeneca investigation and introduce this person to AstraZeneca Global Security.

Organisations must support any AstraZeneca-led investigation into security incidents and permit AstraZeneca or third-party Investigators access to premises, personnel and documentation relevant to the investigation.

Organisations must verify the identity of anyone purporting to be an AstraZeneca Investigator or agent with their existing, relationship manager.

Organisations must ensure incidents are logged and evidence is gathered and retained in a legally compliant manner to permit future investigation.

6 Program security

The following areas must be addressed in the PSP. They should be adapted to fit the nature of the site/process, be based upon the identified risks and be compliant with local regulations.

6.1 Security administration

A description of the administrative processes in place to ensure a secure site/process.

This section should include:

- Organisation and responsibilities.
  The security plan(s) owner and document revision schedule.
  Liaison with law enforcement.
- Employee security education and training programme.

6.2 Policies and procedures

PSPs must articulate the processes used to manage the physical security of all project-related sites. These may be contained within separate SSPs.

This section should include:

- Internal/external access control process.
- Employee and visitor access controls.
- Product shipping, receiving and transport security procedures.
- Restricted areas.
- Intrusion detection systems, alarm monitoring and response.
- Product storage security.
- Secure waste disposal.
- Other procedures as relevant to the facility and its risk profile.

6.3 Personnel security

Organisations are to ensure they have an end-to-end process for secure recruitment, internal security monitoring and end-of-service departure. The aim is to prevent targeted or opportunistic infiltration of the project by hostile parties.

It is acknowledged that legislation and norms in this area vary considerably by jurisdiction. Organisations must demonstrate compliance by locally applicable means, where possible this should include:

- Reference to policies and procedures.
- Candidate recruitment process.
- Pre-employment screening and validation process.
- Employee access determination.
- Rules of behaviour/ conduct.
- Termination procedures (accomplished within 24 hours of leaving, includes termination of all network access.)
- Confidentiality agreements.

7 Physical site security

All sites should have a Site Security Plan SSP. The scope of this plan will vary with the size and complexity of the site. The following measures may not be specifically applicable to all sites. Where this is the case organisations must implement appropriate alternative measures to achieve a high standard of security in the following areas:

1. Secure physical perimeter.
2. Access control and visitor management.
3. Perimeter threat detection and response.

7.1 Security perimeter

- All sites should have a controlled perimeter.
- Perimeters may be delineated by walls, fences, building exteriors etc.
- The form and delay level of the perimeter feature should be determined by the site risk assessment.
- The SSP should articulate what specification the measures use and be linked to the identified risk in the site risk assessment.
- Where it is not possible to maintain a perimeter by means of physical barrier, detection and response measures i.e. CCTV and guard force may be used to supplement the physical measures.

7.2 Access control

- Must have an electronic intrusion detection system with centralizedmonitoring.
- Responses to alarms must be immediate and documented in writing.
- Employ an electronic system to control access to areas where assets critical to the vaccine are located (facilities, laboratories, clean rooms, production facilities, warehouses, server rooms, records storage etc.).
- The electronic access control should signal an alarm notification of unauthorized attempts to access restricted areas.
- Must have a system that provides a historical log of all key access transactions and kept on record.
- Must have procedures in place to track issuance of access cards to employees and the ability to deactivate cards when they are lost or an employee leaves the company.
- Response to electronic access control alarms must be immediate and documented in writing and kept on record.
- Should have written procedures to prevent employee piggybacking access.
- Critical infrastructure (generators, air handlers, fuel storage, etc.) should be controlled and limited to those with a legitimate need for access.
- Must have a written key accountability and inventory process.
- Physical access controls should present a layered approach to critical assets within the facility.

7.3 Employee/visitor identification

- Organisations should issue company photo identification to all employees.

- Photo identification should be displayed above the waist anytime the employee is on company property.
- Visitors should be sponsored by an employee and must present government issued photo identification to enter the property.
- Visitors should be logged in and out of the facility and should be escorted by an employee while on the premises at all times.

7.4 Closed circuit television (CCTV) monitoring

CCTV may be used to supplement or enhance physical security measures. CCTV systems should:

- Be layered (internal/external) CCTV coverage with time-lapse video recording for buildings and areas where critical assets are processed or stored.
- Cover entry and exits to critical facilities, perimeters, and areas within the facility deemed critical to the vaccine project.
- Maintain recordings for a minimum of 30 days (subject to local regulations).
- Be on an emergency power backup system.

7.5 Security lighting

Security lighting may be used to supplement or enhance physical security measures. Security lighting systems should:

- Cover facility perimeters, parking areas, critical infrastructure, and entrances and exits to buildings.
- Have emergency power backup.
- Be sufficient for the effective operation of the CCTV surveillance system during hours of darkness (unless night vision equipped cameras are in use).

7.6 Waste management

Organisations must have controls in place to dispose of waste associated with AstraZeneca products, and materials such that the waste cannot be re-used / re-enter the supply chain.

Materials include: APIs, intermediates, manufacturing / packing equipment, clinical trial materials, branded (identifies as AZ material) packaging/devices, bulk and finished products, waste (solid & liquid)

A waste disposal program should:

- Ensure waste awaiting destruction is stored securely and handled in a manner that prevents unauthorised access.
- Include random inspections of waste containers/waste areas should be conducted and recorded, to detect/deter unauthorised removal of waste.
- Ensure waste destroyed on site is destroyed completely, by appropriate means e.g. packaging by crosscut shredding etc.
- Reconcile the amount/quantity of waste sent for destruction with the amount destroyed.
- Issue certificate of destruction for the quantity/weight of waste sent for destruction and/or observe the destruction process.
- Have a reporting process for deviations.

8 Security operations

8.1 Training

All organisations should have comprehensive staff security training at induction and periodically throughout service. The program should be based upon identified risks. **Organisations should consider preparing specific training in relation to the vaccine program**.

- All staff should be provided security awareness training.
- Training should be mandated in employee annual requirements and recorded
- All staff should receive regular information/cyber security training.

8.2 Manned guarding

Manned guarding requirement should be determined by the site risk assessment. Manned guarding may be used for the day-to-day security management including static guarding, manning of access points and the conduct of screening and searching as required.

The main objectives of a guard force should be:

- Protection of life and safety of those on site.
- Protection of property and premises.
- Prevention of theft including waste materials.
- General crime detection and prevention.
- Incident response.

The guard force may be in-house our outsourced to a third party. Where guarding is provided by a third party the requirements of this standard must implemented by the guard force provider.

Minimum standards for manned guarding should include:

- The guard force should be uniformed and identifiable.
- Have regular training managed through an auditable training plan.
- Have standing instructions for all activities.
- Be trained in appropriate use of force, human rights legislation and locally mandated regulations.

8.2.1 Armed guarding

AstraZeneca prefers armed guarding not be used. Where armed security is used organisation must ensure:

- AstraZeneca is informed of locations and nature of armed security.
- There is a proven requirement (identified in site risk assessment).
- Training, monitoring and auditing standards are enhanced to a commensurate level.

8.3 Information sharing

- Organisations should have formal links with local law enforcement.
- The manager in charge of security should meet with their local contact regularly (annually at a minimum).
- SSPs should record the procedures for receiving and disseminating threat information.

9 Transportation and supply chain security

Organisations must have a supply chain security program in place to mitigate the risks of materials being stolen, tampered with, substituted or illegally diverted and entering the legitimate supply chain. To ensure patients are protected from the dangers of illegally traded medicines and deter criminals from illegally trading.

9.1 Supply chain security procedures

Organisations should have written policies and procedures governing the security of items in transit through the supply chain including:

- Journey Management policy and procedure for all routes.
- Records of all collections and deliveries, retained for a period of not less than 12 months.

9.2 Shipping and receiving areas

Nominated shipping and receiving areas should:

- Have CCTV coverage and an electronic access control system.
- Must have procedures in place to control access and movement of drivers picking up or delivering shipments.
- Formally confirm driver identity.

9.3 Drivers

Drivers should:

- Be trained on specific security and emergency procedures.
- Be equipped with backup communications.
- Identity must be confirmed before the pick-up of any AstraZeneca product.
- Not leave AstraZeneca products unattended, and two drivers may be required for longer transport routes or critical products during times of emergency.

9.4 Vehicles

Vehicles/trailers/containers transporting vaccine related items should:

- Be stored in a secure location when not in use.
- Trailers should have solid top, hard sided with lockable cargo doors for pharmaceutical products.
- Containers/trailers/vehicles should be equipped with an immobilisation device and GPS vehicle location tracking when transporting AstraZeneca materials.
- Tracking should:
    - Be monitored 24/7.
    - Have set reporting interval time.
    - Have an untethered alert.
    - Have an “idle” alert.
    - Use geo-fenced alerts to detect route deviation.
- For high risk routes vehicles should be provided with two-way communication.

9.5 Transport routes

Transport routes should:

Be pre-planned and not deviated from except when approved or in the event of an emergency. Have contingency plans in place for reporting unscheduled events (e.g. stops, delays, route deviation).

- be continuously evaluated based upon new threats, significant planned events, weather, and other situations that may delay or disrupt transport.
- Where practicable are journeys completed without break, were breaks are made, vehicles should be parked in designated secure areas, locked with alarm active.

9.6 Product security in transit

- AstraZeneca products must be secured with tamper resistant seals during transport, and the transport trailer must be locked and sealed.
- Tamper resistant seals must be verified as “secure” after the product is placed in the transport vehicle.
- AstraZeneca products should be continually monitored by GPS technology while in transport, and any deviations from planned routes should be investigated and documented.
- Contingency plans should be in place to keep the product secure during emergencies such as accidents and transport vehicle breakdowns.

9.7 Locks and Seals

- Tamper resistant, uniquely numbered security seals should be used for all AstraZeneca and vaccine related products.
- If exporting to the US or EU, seals must meet or exceed current PAS ISO 17712.
- Seals should be classed as accountable items and securely stored.
- Seal inventory logs and shipping documents should be periodically reconciled.

10 Cyber Security

All parties must maintain cyber security administrative, technical, and physical measures, controls, tools, systems, policies and procedures in accordance with Good Industry Practice and the attached bundle of AZ Cyber Security Policies and Standards to manage the risks posed to the security to prevent and minimise the impact of security incidents and to ensure the continuity of their business and the services provided.

Policy / Standard
Corporate Information Technology Usage Policy
Information Technology Security Policy
Access Management Standard
End User Computing Device Security Standard
Secure Information Management Standard
Security in Contracts
Data Sanitization Standard
IT Network Design, Configuration and Hardening Standard
IT Software Design, Configuration and Hardening Standard
Monitoring & Logging
Secure Electronic Data Transfer
User ID & Password Configuration Standard
Vulnerability Management Standard
Removable Media Usage Standard

To identify and obtain copies of the insider threat and cyber security requirements standards relevant to your organinsation and for implementation advice please contact: AstraZeneca Cyber Security Governance SecurityGovernance@astrazeneca.com