**AGREEMENT #: W15QKN2191003 -FLOWDOWN REQUIREMENTS FOR SUBCONTRACTS**

**(Appendix A)**

*This appendix applies to any subcontracts in support to AstraZeneca prime agreement with US Government W15QKN-21-9-1003 .*

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 an Other Transaction Agreement ("OTA") No *W15QKN-21-9-1003* for the United States Government.

## 1. GOVERNMENT SUBCONTRACT

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

The work required under this Agreement will be performed in support of AstraZeneca's OTA with Government. As a Subcontractor under the OTA, Subcontractor must meet certain AstraZeneca's requirements under its prime agreement with the US 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 W15QKN-21-9-1003 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.

## 2. CONFIDENTIAL INFORMATION

A. "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.
B. AstraZeneca representative and the Subcontractor may, by mutual consent, identify elsewhere in this Agreement specific information and/or categories of information which the AstraZeneca or Government will furnish to the Subcontractor or that the Subcontractor is expected to generate which is confidential. Similarly, the AstraZeneca representative and the Subcontractor may, by mutual consent, identify such Confidential Information from time to time during the Period of Performance. Failure to agree will be settled pursuant to the relevant dispute clauses in the Agreement.
C. 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.

D. The Receiving Party shall not directly or indirectly, divulge or reveal to any person or entity any Confidential Information of another Party without the Disclosing Party's prior written consent, or use such Confidential Information except as permitted under this Agreement. Confidential Information shall be subject to the same prohibitions on disclosure as provided for under FAR Part 24.202. Further, any reproduction of Confidential Information or portions thereof that is disseminated within the Government or AstraZeneca or Subcontractor, shall be shared strictly on a need to know basis for the purposes of this Agreement and is subject to the restrictions of this provision. In addition to the above, Confidential Information is subject to the protections of the Trade Secrets Act as well as any other remedies available under this Agreement or the law.
E. Such obligation of confidentiality shall not apply to information which the Receiving Party can demonstrate through competent evidence: (i) was at the time of disclosure in the public domain; (ii) has come into the public domain after disclosure through no breach of this contract; (iii) was known to the Receiving Party prior to disclosure thereof by the Disclosing Party; (iv) was lawfully disclosed to the Receiving Party by a Third Party which was not under an obligation of confidence to the Disclosing Party with respect thereto; or (v) was approved for public release by prior written permission of the Disclosing Party.
F. 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.
G. AstraZeneca will reflect the result of internal coordination with appropriate program and legal officials.
H. The provisions of paragraph (D) of this Article shall not apply to conflicting or overlapping provisions in other Federal, State or local laws.
I. The obligations of the Receiving Party under this Article shall continue for a period of seven (7) years from conveyance of the Confidential Information.
J. 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 this Article flows down to the relevant sub-agreement, and such entity agrees to be in substantial compliance with this Article.
K. 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 Agreement W15QKN-21-9-1003. 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.

## 3. 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.

## 4. AUDITS

Until such time as all doses have been delivered under this Agreement, and in no event after expiration of the Period of Performance, audits under this Agreement may include Government Quality Assurance audits – periodic, ad hoc or for cause – of AstraZeneca or sub-agreement holders' facilities included in the AZD1222 supply chain. AstraZeneca or the Government will provide notification of a periodic or ad hoc audit at least fourteen (14) calendar days prior to the intended audit date and all parties will work in good faith to accommodate the audit and determine scheduling. Audits performed for cause will not require notification by the Government. In all audits, the Government will comply with the Person in Plant requirements set forth in Article "Person in Plant".

## 5. PERSON IN PLANT

AstraZeneca or the Government may request to have a government representative in place at Subcontractor's facility, with no fewer than fourteen (14) calendar days' advance notice of the desired date for that person to be in place. The name, role, scope and duration will be mutually agreed between the Parties in writing in advance. The Government representative will adhere to the agreed scope and to the Subcontractor's policies, procedures and instructions at all times. As determined by federal law, no Government representative shall publish, divulge, disclose, or make known in any manner, or to any extent not authorized by law, any information coming to him in the course of employment or official duties, while stationed in a Recipient plant.

If considered for cause, AstraZeneca and/or the Government may place representatives in place at Subcontractor's facility, with no fewer than 3 (three) business days' advance notice of the desired date for the person(s) to be in place, subject to applicable COVID protocols. The names, roles, scope, and duration will be provided to the Subcontractor in advance. The Government representative will adhere to the Subcontractor's policies, procedures and instructions regarding facility regulations at all times. As determined by federal law, no Government representative shall publish, divulge, disclose, or make known in any manner, or to any extent not authorized by law, any information coming to him in the course of employment or official duties, while stationed in a Subcontractor's plant.

## 6. COMPTROLLER ACCESS FINANCIAL RECORDS AND REPORTS

Subcontractor shall maintain adequate records to account for all costs incurred under this Agreement for which Subcontractor seeks reimbursement. Subcontractor's relevant financial records are subject to examination or audit by or on behalf of the AstraZeneca, Comptroller General, Contracting Activity AO, or other Government Official for a period not to exceed three (3) years after expiration of the term of the Agreement. AstraZeneca, the Comptroller General, AO or designee shall have direct access to sufficient records and information of any party to this agreement or any entity that participates in the performance of this agreement to ensure full accountability for all funding under this Agreement. Such audit, examination or access shall be performed during business hours on business days upon prior written notice and shall be subject to the security requirements of the audited party. Any audit required during the course of the program may be conducted by AstraZeneca, the Comptroller General or other Government Official using Government auditors or, at the request of Subcontractor's external CPA accounting firm at the expense of the Subcontractor.

The Performer shall include this Article, suitably modified to identify the Parties, in all subcontracts or lower tier agreements entered into solely in connection with this Agreement.

## 7. FOREIGN ACCESS TO DATA.

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

in performing this Agreement.

**8. 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 AZD1222 (*i.e.*, would not apply more broadly to AstraZeneca's or Subcontractor's other programs, such as its manufacturing platform), except as authorized by Government personnel and AstraZeneca 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.

**9. FINANCIAL DISCLOSURE BY CLINICAL INVESTIGATORS**

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

**10. ACCESS AND GENERAL PROTECTION / SECURITY POLICY AND PROCEDURES**

This standard language text is applicable to ALL employees working on critical information related to Operation Warp Speed (OWS) with an area of performance within a Government controlled installation, facility or area. Employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). The performer also shall provide all information required for background checks necessary to access critical information related to OWS, and to meet Government installation access requirements to be accomplished by installation Director of Emergency Services or Security Office. The workforce must comply with all personnel identity verification requirements as directed by the Government and/or local policy. In addition to the changes otherwise authorized by the changes clause of this agreement, should the security status of OWS change the Government may require changes in performer security matters or processes. In addition to the industry standards for employment background checks, the Subcontractor must be willing to have key individuals, in exceptionally sensitive positions, identified for additional vetting by AstraZeneca and the United States Government.

**11. SCIENTIFIC PUBLICATIONS AND PRESS RELEASES**

A. Subcontractor shall not make, or permit any person to make, any public announcement concerning the existence, subject matter or terms of this Agreement, the transactions contemplated by it, or the

relationship between the Subcontractor and AstraZeneca and Government hereunder, without the prior written consent of the other, such consent not to be unreasonably withheld or delayed, except as required by law, any governmental or regulatory authority (including, without limitation, any relevant securities exchange), any court or other authority of competent jurisdiction.

B. Notwithstanding the foregoing, Subcontractor and (its upstream licensor) retains the right, but not the obligation, to prepare and submit scientific publications and release information to the public about its COVID-19 development program, without AstraZeneca's and the Government's consent or involvement. The Subcontractor shall inform AstraZeneca when any abstract article or other publication is published, and furnish a copy of it as finally published.

C. 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.

D. 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.

E. The Subcontractor shall include this Article, including this clause and section (d) 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:

E. "This project has been funded in whole or in part by the U.S. Government under Agreement No. W15QKN21-9-1003. The US Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon."

## 12. 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, 50, 54 and 56.

D. All clinical sites and IRBs utilized in the clinical trial described in the Statement of Work are required to register with the Office for Human Research Protections (OHRP) and receive Federal Wide Assurance (FWA) numbers in accordance with human subject protections regulations 45 C.F.R 46.103.

## 13. 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 its Sub-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.

C. Audits of Sub-agreement Holders' Facilities: The Subcontractor will inform AstraZeneca of upcoming, ongoing, or recent audits/site visits conducted by Subcontractor of sub-agreement holders as part of the weekly communications, including goals and agenda. The Government reserves the right to participate in the audits.
Upon completion of the audit/site visit the Subcontractor shall provide a report capturing the findings, results and next steps in proceeding with the sub-agreement holder if action is requested by Subcontractor of the subagreement holder to address areas of non-conformance to FDA regulations.

## 14. SUBAWARDS

1. AstraZeneca acknowledges that, in order to combat the global pandemic and launch AZD1222 as quickly as possible, Subcontractor has entered into a number of contracts prior to the Execution Date, and the Government agreed that it will not require these contracts to be renegotiated. Therefore, except as otherwise expressly set forth in this Article 15, any provision requiring Subcontractor to flow-down an obligation to its subawardees/sub-agreement holders will apply only to sub-agreements executed by Subcontractor following the Execution Date of this Agreement.

2. For clarity, as detailed within the Articles themselves, the following Articles require flow-down to sub-agreements/contracts executed before the Execution Date:

(i) Article 2: Confidential Information; Subcontractor acknowledges that confidential information will not be provided to sub-agreement holders unless or until Article 2 flows down to the relevant sub-agreement, and such entity agrees to be in substantial compliance with this Article

(ii) Article 17: Security Plan per Exhibit B (to be provided by AZ)
(iii) Article 15: Prohibition on the Use of Certain Telecommunications and Video Surveillance Services or Equipment must be flowed-down to all subagreements/contracts as set forth in FAR 52.204-25, whether

executed before or after the Execution Date.
(iv) Article 6: Comptroller Access Financial Records and Reports

## 15. PROHIBITION ON THE USE OF CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

Use of Covered Telecommunications. FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment is hereby incorporated.

This clause shall be flowed-down to all sub-agreements/contracts as set forth in FAR 52.204-25, whether executed before or after the Execution Date

a) Definitions. As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE

Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) 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

(6) 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 Subcontractor 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 Subcontractor is notified of such by a subcontractor at any tier or by any other source, the Subcontractor shall report the information in paragraph (d)(2) of this clause to the AstraZeneca Representative, unless elsewhere in this contract or agreement are established procedures for reporting the information; in the case of the Department of Defense, the Subcontractor shall report to the website at https://dibnet.dod.mil.

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

## 16. HEALTH RESOURCES PRIORITIES AND ALLOCATIONS SYSTEMS (HRPAS) PRIORITY RATING (Removed effective 6/4/2021)

## 17. SECURITY PLAN

(1) The Subcontractor agrees to implement security plans aligned to the standards outlined in Section 17 (2) (provided upon AstraZeneca AZD1222 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 17 (2).

However, AstraZeneca acknowledges that, in order to combat the global pandemic and launch AZD1222 as quickly as possible, the Subcontractor 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 AZD1222 Project Security Standard**

AstraZeneca
Global Security

# AstraZeneca AZD1222 Project Security Standard

## 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 isconducted.

## 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.

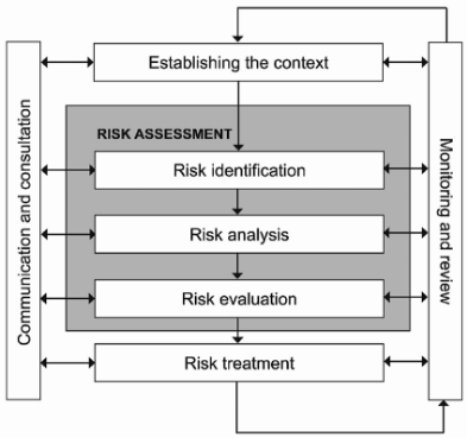


Figure 1 ISO 31000:2009

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 AZD1222 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 centralized monitoring.
- 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