Appendix A

Coalition for Epidemic Preparedness Innovations (CEPI) – AstraZeneca UK Limited Agreement for Outbreak Response to Novel Coronavirus (COVID-19) dated June 4, 2020—Flow down of Terms and Conditions for Subcontracts

This appendix applies to any subcontracts in support to the AstraZeneca prime agreement with CEPI titled "Agreement for Outbreak Response to Novel Coronavirus (COVID-19)" dated June 4, 2020.

In this Appendix A, "Subcontractor" means a contract manufacturer, contractor or subcontractor engaged by AstraZeneca to perform activities contemplated by a Manufacturing Plan established under the Agreement for Outbreak Response to Novel Coronavirus ("COVID-19") dated June 4, 2020.

Subcontractor understands and acknowledges that AstraZeneca is performing an Agreement for Outbreak Response ("CEPI Agreement") for the Coalition for Epidemic Preparedness Innovations.

"Subcontract" means this "Agreement". "Subawardee" means any contractor that has been contracted by Subcontractor to provide goods and services in support of this Agreement.

FOUNDATION SUBCONTRACT

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

The work required under this Subcontract will be performed in support of AstraZeneca's CEPI Agreement. As a Subcontractor under the CEPI Agreement, Subcontractor must meet certain of AstraZeneca's requirements under its prime agreement with CEPI. Subcontractor confirms that it is eligible to perform subcontracting work funded by the Coalition for Epidemic Preparedness Innovations (CEPI) and agrees with the Terms & Conditions/Flow downs listed in this Appendix. Further, to the extent the Subcontractor must enter into subawards to fulfill requirements of this Agreement or any service hereunder the CEPI Agreement 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 CEPI 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 CEPI 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.

Subcontractor agrees to comply with the terms and conditions set forth in this Appendix, in each case, to the extent related to (i) Product intended for distribution to GAVI (or to any other designee of CEPI or GAVI), including any Capacity Reservation Fee in respect thereof or (ii) funds provided by CEPI to AstraZeneca under the CEPI Agreement. AstraZeneca will identify any Product Schedules or Capacity Reservation Fees meeting the criteria set forth clauses (i) or (ii) of in the immediately preceding sentence. For purposes of this Appendix, the "CEPI Agreement" means that certain Outbreak Response Funding Agreement, dated June 4, 2020, between CEPI and AstraZeneca.

1. Disclosure of Confidential Information. AstraZeneca may disclose Confidential Information of Subcontractor to CEPI pursuant the terms of the confidentiality provisions of the CEPI Agreement. To the extent that AstraZeneca shall disclose any non-public information of CEPI or to Subcontractor, Subcontractor hereby agrees to be bound by the confidentiality provisions of the CEPI Agreement, which are attached hereto as Addendum One.

2. Assignment or Novation. In the event that the CEPI Agreement is terminated by CEPI, at CEPI's request, this Agreement may be assigned or novated to CEPI, and until such assignment or novation is effective, AstraZeneca shall hold the Agreement on trust for CEPI. AstraZeneca will notify Subcontractor of any such request by CEPI. In the event of any such assignment or novation, a license granted by AstraZeneca pursuant to the CEPI Agreement shall remain in effect after such assignment and novation during the Term.

3. Use of Capacity Reservation. In the event AstraZeneca does not utilize any portion of any Capacity Reservation to the extent reserved with funds provided by CEPI to AstraZeneca under the CEPI Agreement, then prior to Subcontractor reselling such Capacity, CEPI shall have the right, but not the obligation, to use the unutilized portion of such Capacity Reservation for production of a Third Party product designated by CEPI, at CEPI's cost, on terms to be agreed between CEPI and Subcontractor.

4. Use of Funds. Any payment by AstraZeneca to Subcontractor of funds provided by CEPI to AstraZeneca under the CEPI Agreement, including any Capacity Reservation Fee in respect thereof, shall be used in accordance with CEPI Cost Guidance. For purposes hereof, "CEPI Cost Guidance" means CEPI's guidance document regarding eligible direct and indirect costs, non-eligible costs, and valuing in-kind contributions, attached hereto in Exhibit A.

5. Record Keeping. Subcontractor shall keep accurate records of its activities and expenditures under the Agreement and retain them for five (5) years after expiration or termination of the CEPI Agreement. AstraZeneca will notify Subcontractor of the date of expiration or termination of the CEPI Agreement.

6. Access to Financial Records. During the term of the CEPI Agreement and for a period of five (5) years after expiration or termination thereof, AstraZeneca or CEPI, or its designee (which shall be an internationally recognized certified public accounting firm, not engaged on a contingent basis), and at AstraZeneca or CEPI's sole expense, shall access to inspect and audit Subcontractor's financial records, including on-site access at Subcontractor's discretion or if electronic access is not otherwise made available by Subcontractor, upon at least fifteen (15) business days' advance notice, provided that (i) AstraZeneca or CEPI (or its designee) shall use reasonable endeavors not to conduct any such audit more than once during any consecutive 12-month period and where the same information for the same period has previously been audited under this Sub-Clause, AstraZeneca or CEPI shall first provide those prior audit results to the party seeking the audit in advance of the subsequent audit. Such inspections shall be conducted during normal operating hours in a manner to minimize disruption to Subcontractor's business.

7. Compliance.

7.1 Compliance with Applicable Laws. Subcontractor shall comply with the laws and regulations that are applicable to its activities and operations under this Agreement (including with respect to the use of funds).

7.2 CEPI's Third Party Code. For purposes hereof, the "Third Party Code" or the "Code") means the periodically updated, consolidated statement of CEPI's values, principles, policies and procedures attached hereto in Exhibit A. AstraZeneca shall notify Subcontractor of material changes to the Code as soon as reasonably practicable after AstraZeneca is notified of such changes by CEPI. To the extent applicable to the activities contemplated by the Agreement:

7.2.1 Subcontractor acknowledges the statement of CEPI's values in Section 1 of the Code.

7.2.2 Subcontractor acknowledges AstraZeneca's and CEPI's expectation that Subcontractor shall adhere to business practices, ethical principles and legal requirements that are at least substantially similar to those described in Sections 2 to 10 of the Code.

7.2.3 Subcontractor shall comply with the requirements for reporting compliance concerns and misconduct to AstraZeneca, for further reporting to CEPI (Sections 4 and 11 of the Code).

7.2.4 Subcontractor shall cooperate as may be requested by AstraZeneca or CEPI in the submission of information related to activities contemplated by this Agreement and expenditures in accordance with the International Aid Transparency Initiative (Section 12 of the Code).

7.2.5 Subcontractor shall comply with CEPI's Equitable Access Policy, which is attached hereto in Exhibit A.

7.2.6 Subcontractor shall comply with CEPI's Animals in Research Policy, which is attached hereto in Exhibit A.

7.2.7 Subcontractor shall comply with CEPI's Clinical Trials Policy, CEPI's Managing Conflicts of Interest Policy, CEPI's Scientific Integrity Policy and CEPI's Travel Policy and CEPI's Expenses Policy, which are attached hereto in Exhibit A.

7.2.8 Subcontractor shall comply with the provisions related to Procurement/Sub-Contracts (Section 14 of the Code) and to Grant-Making/Sub-Grants (Section 15 of the Code) and if requested, shall sign the declaration regarding such compliance provided by CEPI.

7.3 Compliance Audit. AstraZeneca or CEPI, or an auditor appointed by AstraZeneca or CEPI, shall be entitled to audit Subcontractor's performance of its compliance obligations under this Agreement, upon reasonable notice.

8.0 CEPI Access. AstraZeneca may permit CEPI to exercise and enforce AstraZeneca's and CEPI's rights under this Appendix, directly with Subcontractor.

9.0 Security Plan

The Subcontractor agrees to implement security plans aligned to the standards outlined in Exhibit B (provided upon AZ 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 Exhibit[B.

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. 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.

[Addendum One– Confidentiality Provisions of CEPI Agreement]

To be attached: [Exhibit A – CEPI Third Policy Code of Conduct and Applicable Policies]

[Exhibit B -- AZ1222 Project Security Standard]

==========

Addendum One: **CONFIDENTIALITY**

Confidential Information. Confidential Information means non-public information disclosed by one Party to the other. For avoidance of doubt, for so long as none of the exceptions set forth in "Confidentiality Limitations" herein, Cost Of Goods, production, supply, pricing and sales of Project Vaccine shall be deemed Confidential Information of AstraZeneca, provided however, that CEPI shall have the right to utilize and disclose such Confidential Information in a manner that anonymizes AstraZeneca's identity and information by aggregating it with similar information from other of CEPI's awardees or third parties. Each Party undertakes that during the term of this Agreement and for so long as a Party is in possession of the other Party's Confidential Information , it shall keep confidential and not disclose the other Party's Confidential Information to any person other than its employees, agents, consultants, contractors, professional advisers, Sub-Contractors and regulatory authorities and, in the case of CEPI, its funders and Assessors, who have a need to know and agree to be bound by the confidentiality provisions of this Agreement. Each Party shall take commercially reasonable precautions to protect against unauthorized disclosure.

Confidentiality Limitations. Confidential Information shall not include: (a)information already known to the receiving Party and which is not subject to preexisting obligations of confidentiality; (b)information that is independently developed by the receiving Party; (c)information that is or becomes part of the public domain other than by unauthorized disclosure by receiving Party; (d)information properly obtained by the receiving Party from a source that, to the best knowledge of the receiving Party after reasonable investigation, is not bound by a confidentiality obligation to the disclosing Party; and (e)information to the limited extent that is required to be disclosed by a competent legal authority; provided, that where it is free to do so, the receiving Party shall where legal to do so (i) give notice of such disclosure to the disclosing Party as soon as reasonably practicable, (ii) inform the disclosing party of the full circumstances of the required disclosure and the information that must be disclosed, (iii) take all such steps as may be reasonable and practicable in the circumstances to agree the contents of the required disclosure with the disclosing Party before it is made, (iv) consult with the disclosing Party as to possible steps to avoid or limit the required disclosure or to seek confidential treatment thereof, (v) gain assurances as to confidentiality from the body or authority requiring the disclosure, (vi) where the disclosure is by way of public announcement, agree the wording of such announcement with the

disclosing Party before it is made and (vii) cooperate with, and provide reasonable assistance to, the disclosing Party to the extent it seeks to bring any legal or other proceedings to challenge the validity of the requirement to disclose such information, otherwise secure a protective order to prevent any such disclosure.

AstraZeneca
Global Security

AstraZeneca 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.

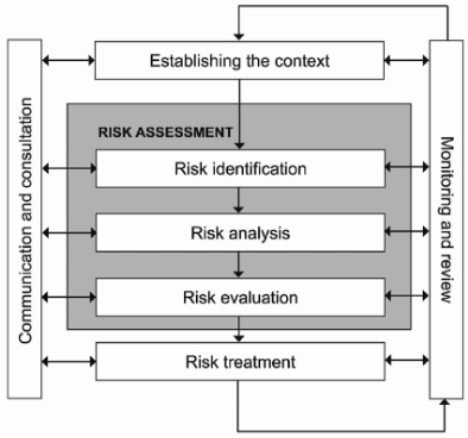

Figure 1 ISO 31000:2009

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 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