ASTRAZENECA GLOBAL POLICY
SAFEGUARDING COMPANY ASSETS AND RESOURCES

THIS POLICY SETS OUT THE REQUIREMENTS FOR SAFEGUARDING COMPANY ASSETS AND RESOURCES TO PROTECT PATIENTS, STAFF, PRODUCTS, PROPERTY AND INFORMATION.

Who is this Policy for?

- **All staff have a responsibility for respecting Company assets and resources and acting appropriately;**
- **Managers are accountable for ensuring appropriate internal controls and training are in place to manage assets and resources in accordance with the requirements set out in this Global Policy.**

KEY PRINCIPLES FOR MANAGING COMPANY ASSETS AND RESOURCES

The Company is committed to managing its assets and resources in a responsible manner. It does this on behalf of its shareholders and to protect patients, staff, products, property and information. This is achieved through line accountability that clarifies to every individual their role in minimising losses and disruption, and safeguarding Company integrity and reputation. This Global Policy, associated standards and procedures specify the requirements for: the management of assets and resources; the maintenance of internal financial, regulatory and operational controls; the management of significant risks; and the protection of the business in the face of significant events.

- We must manage assets efficiently and effectively so that the Company realises their full value and complies with its obligations;
- We must identify and manage our information assets using good information practice;
- We must operate and maintain a robust internal financial, regulatory and operational control system that is designed to promote efficiency, prevent fraud and help ensure the reliability of financial statements and compliance with applicable laws and standards;
- We must identify, prioritise, manage and report risks to Company assets, employees or patients so that we achieve our business objectives, comply with legal requirements and safeguard shareholder value;

- We must be prepared to the fullest extent practicable to respond to significant events so that our critical business processes are maintained.

MANAGING ASSETS AND RESOURCES

1. The Company is committed to the effective and compliant management of its assets and resources to meet the following objectives:

   - Realise the full value of assets and resources to deliver business objectives, making a meaningful difference to patient health;

   - Ensure compliance with legal requirements and safeguard shareholder value by protecting assets and resources;

   - Manage assets and resources in an efficient manner that ensures effective use and facilitates sound decision making;

   - Work to ensure that our external partners manage our assets and resources in a manner compliant with this policy.

   Related expectations can also be found in the following Global Polices: Data Protection & Privacy; Legal & Intellectual Property; and Safety, Health and Environment; Providing Information about our Products; Business Travel.

MANAGING INFORMATION AS AN ASSET

2. **Good information practice.** For the purposes of this policy information is defined as “information that the Company or contracted partner creates or handles, in all formats including physical, electronic or verbal, or the use of other knowledge in the course of Company business”.

   To that end, this policy specifies the six key principles to be employed when managing information. The Company’s six principles of Good Information Practice and their expected business outcomes are:

   Accountability: Accountable people recognising information as an asset.
   By agreeing and maintaining clear ownership and accountability for information we ensure appropriate levels of personal responsibility and management oversight throughout the information lifecycle.

   Integrity: Accurate information with trustworthy sources.
   By making sure that information is accurate, relevant and trustworthy we ensure it supports the integrity of decision making and end-to-end business processes.

   Retention: Keep what is needed, dispose of the rest.
   By keeping only information that supports well understood compliance and business objectives and disposing of what we no longer need in a timely way, we retain the information assets we need without incurring

unnecessary business risk and cost.

Compliance: Standards are understood and met.
By assuring that information is compliant with the Company's legal, regulatory, fiscal, ethical and operational obligations we help to maintain our licence to operate and achieve our reputational goals.

Availability: Accessible information enabling people.
By making the right information available to the right people, at the right time, we improve our effectiveness and the quality of decision-making and enhance our ability to innovate for business value.

Protection: Information is safeguarded through processes that are secure and understood. By agreeing and maintaining the appropriate access and other controls for information we ensure that the varied interests of relevant stakeholders including patients, shareholders and employees are protected.

3. **Company records.** Line managers are accountable for the management of Company records created during the course of our business activities throughout their entire lifecycle, including creation, use, management, storage and retrieval, archiving and disposal.

   It is the Company's policy to: value records as corporate assets; retain records required by law or regulation or having business or historical value; manage records efficiently; protect and hold records according to company standards; and dispose of records at the appropriate time as stipulated in the Global Retention and Disposal (GRAD) Schedule Standard.

   - Recorded information represents official business records regardless of media form or other format characteristics, when created or received by the Company and considered as evidence of its functions, decisions, policies, operations and other activities.

   - Records are important corporate assets to be safeguarded. Company records must have the appropriate level of protection from unauthorized use, disclosure, damage or loss.

   - Legal Holds supersede any legal, regulatory and business retention requirements identified in the GRAD Schedule Standard and we must ensure that all versions and copies of records on Hold are preserved until the associated Hold is removed.

   - Adherence to efficient records management practices will help assure Company information is protected, accurate, useful and readily accessible whenever it is needed.

4. **Information security principles.** All Company and third party information for which the Company is responsible must be protected to preserve its confidentiality, integrity and availability, including the proper handling of information by third parties.

   All staff must also comply with the Global Policy: Communications and supporting standards. Staff are responsible for handling information in ways appropriate to its sensitivity and any specific requirements for its protection.

   Specific requirements for data protection and privacy are stated in the Global Policy: Data Protection and Privacy.

   When sharing information internally and with third parties, applicable global standards or procedures must be followed, and steps taken proportionate to the sensitivity of the information, to ensure that it will be properly protected in storage, in transit and by the recipient.

   All staff must comply with the Group Standard Disclosure. It covers all disclosures of inside information by the Company. Inside information is any precise, non-public information relating to the Company's business or financial position that, if it were made public, could have a significant effect on the price of AstraZeneca PLC shares.

5. **Computer Usage.** All information services must be provided and operated in a manner consistent with the IS Policy. All computer usage, including the use of computers, networks and all other types of equipment and technology to handle information, must comply with the Computer Usage Policy.

6. **Copyright.** To ensure that all third party information is used in a legal manner:

   - All staff have a responsibility to use information only in a way that is in compliance with copyright laws and with any licences and agreements into which the Company has entered for the use of copyright-protected materials;

   - All staff must comply with the Global Standard on Use of Third Party Information when using third party copyright-protected works.

7. **Competitive intelligence.** All activities to obtain information on competitor companies and products must be legal and ethical.

   - All staff and others working on behalf of the Company must not seek information that constitutes trade secrets of a third party without the authorisation of such party.

   - If trade secrets are offered to a member of staff, they must be refused and the Legal Department should be consulted with respect to possible follow-up actions.

- If unsolicited trade secrets are received, the Legal Department should be consulted and, when appropriate, the owner of the information should be notified and any documents received returned to the owner.

- If a conversation containing trade secrets is inadvertently overheard, staff should inform their manager and the information should not contribute to significant business decisions.

- Staff should not be asked to provide, nor should they offer, any information that would reasonably be considered as trade secrets by their previous employers.

MANAGING INTERNAL FINANCIAL, REGULATORY AND OPERATIONAL CONTROLS

8. Line Managers are accountable for the development, implementation and ongoing operation and monitoring of appropriate financial controls for each relevant function to ensure the following objectives:

    - Effective and efficient operation of the applicable SET/functional area;

    - Financial reporting that operates with integrity, reliability, accuracy, transparency and timeliness;

    - Compliance with applicable laws, regulations and standards.

    The Company will operate internal control processes consisting of inter-related components:

    - A control environment that encompasses values, processes and skills to ensure that financial transactions are recorded and reported accurately and that includes:

        - A commitment to integrity, ethical values and competence;

        - Management's philosophy and operating style;

        - Delegation of authority and responsibility;

        - Participation and direction by the Board of Directors of AstraZeneca PLC (the Board).

    - Control activities that:

        - Include the establishment of policies and procedures to ensure management's directives are carried out;

        - Encompass a range of activities, including approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

- Information and communication processes that ensure pertinent information is identified, captured and communicated in a form and timeframe that enables staff to carry out their responsibilities;

- Information systems that are designed and established to produce reports containing operational, financial and compliance-related information to operate and control the business;

- Monitoring that assesses the effectiveness of the internal control system over time through ongoing monitoring activities, separate evaluations or a combination of the two;

- Reporting of deficiencies in the internal control system to line management, the Audit Committee and the Board, and corrective actions to ensure continuous improvement of the system.

9. **Anti-fraud principles.** The Company does not tolerate fraud. We will take all reasonable steps to prevent the Company from becoming a victim of fraud, and we will not tolerate any fraud perpetrated in our name.

   Where fraud is detected, the Company will take necessary steps to stop it immediately, mitigate any resulting loss or damage and evaluate whether corrective actions or additional controls are necessary to prevent future fraud (and if so, to implement them expeditiously).

   When the Company has been a victim of fraud, the Company shall seek to recover whatever has been lost as a consequence of the fraud. The Company shall consider taking legal action against the perpetrators of fraud, whether they are staff or external to the Company.

   Any potentially improper action against Company resources must be reported promptly through recognised channels and investigated.

   Staff who commit fraud are subject to disciplinary action up to and including dismissal.

10. **Procurement principles.** For each SET/functional area, line managers are accountable for ensuring that:

    - The SET/functional area meets its business objective of delivering best value spend management across the Company in line with the needs and priorities of the business by leveraging and linking appropriate Company resources and effectively utilising our suppliers' capabilities;

    - We protect the Company's commercial and legal rights;

    - All purchasing activities:

- Are approved within the authority limits delegated by the Board and the SET;

- Have suitable segregation of duties to ensure that procurement requisition, procurement commitment, and invoice approval have appropriate decision-making controls in place;

- Value delivered is measured in terms of the quality of goods and services purchased and the total ownership costs;

- The optimum balance between local or functional business needs and overall corporate benefit is achieved;

- Processes and procedures designed to ensure compliance with this policy are implemented and followed by SET areas (e.g. the Procurement Policy and Internal Governance Framework);

- High standards of professional ethics and personal integrity are maintained in line with the AstraZeneca Code of Conduct, including the sections on 'Preventing Bribery and Corruption' and 'Avoiding Conflicts of Interest'. We must operate within an ethical procurement framework that is compliant with Company SHE policies, the financial control framework and the Responsible Procurement Standard;

- Suppliers are treated with appropriate respect.

MANAGING RISK

11. The Company is committed to effective risk management to meet the following objectives:

    - Safeguard shareholder value and protect the company's assets and resources;

    - Help achieve business objectives by guiding specific management decisions both strategic and operational;

    - Ensure both compliance with applicable legal requirements and effective corporate governance.

    This policy and associated procedures specify the requirements for the identification, prioritisation, management and reporting on the risks faced by the Company. All types of risk are covered within the scope of this policy, including long term value/strategic, financial control, compliance and reputational risks and shorter term performance/operational risks impacting the long term business plan and annual budgeting cycle.

    The purpose of effective risk management is to ensure that:

- Accountabilities and responsibilities for risk management and oversight are clearly understood;
- Significant risks to corporate and business strategies are understood and effectively managed;
- The risks of non-compliance with policies and applicable laws and regulations are understood and adequately controlled;
- The impact of risks is assessed by measuring how a particular risk might adversely affect the value of the business in the event the risk is realised;
- Mitigation and business resilience plans for significant risks are adequately specified, executed and monitored;
- Reporting on risks and how they are controlled is accurate, relevant and timely;
- Appropriate escalation of potential risks is achieved using clear criteria, integrated into business processes.

The Company provides guidelines that describe the risk management process, the roles and responsibilities that enable its successful operation and the annual and quarterly risk process.

PREPARING FOR, AND RESPONDING TO, SIGNIFICANT EVENTS

12. **Business resilience.** The Company is committed to being prepared to the fullest extent practicable to continue critical business processes in the event of a business disruption, and to managing the company's response to any event that may negatively impact the reputation of AstraZeneca or its products.

    Business Resilience relies on having the specific plans in place to minimise the impact and potential disruption to the business from key business threats identified during business risk assessment processes.

    Line managers are accountable for readiness and response planning, for having the appropriate capabilities, and for providing assurance for the adequacy of the plans within SET and Functional areas. The relevant SET member is accountable for providing assurance for the adequacy of the plans.

    Collectively, Business Resilience is comprised of some or all of the following, depending on the nature of the business activities and the threats to them:

    Business continuity: Business Continuity Management Planning addresses the continuity of critical business processes in the event of

significant business disruptions affecting people, workspace and/or technology. SET members are responsible for identifying critical processes through risk assessment and for assigning owners to these processes. Critical process owners are responsible for developing, testing and maintaining business continuity plans appropriate to their part of the business.

Crisis management: Crisis Management is a series of senior management-led activities designed to address, manage and resolve or terminate, quickly and effectively, any significant event that has the potential to negatively affect the business or its reputation. Crisis Management is geographically aligned and escalated to Group based on severity. Specific requirements and responsibilities relating to the preparation for, and management of, a crisis are established in the Crisis Management Standard.

Disaster recovery: Disaster Recovery Planning addresses the recovery of critical computerised systems that support the Business. The AZ IS function has the primary accountability for disaster recovery.

Emergency response: Emergency Response is the collective action taken at a site to stabilise incidents that have the potential to injure people, damage or contaminate property or interrupt business operations.

13. **Counterfeit medicines.** The Company will seek to protect patients from the dangers of counterfeit or illegally traded medicines by:

    - **Building strong, collaborative partnerships** to strengthen enforcement and raise awareness. We work with other pharmaceutical companies, our supply chain partners, governments, and law enforcement agencies to raise awareness of the issue and implement effective solutions;

    - **Securing our products** through pack security features to aid verification and deter copying, and improving the security of the end-to-end supply chain;

    - **Working in enforcement** to combat illegal activity through professional investigation of reported suspicions.

    Staff who are aware of suspicions relating to possible counterfeiting or illegal trade of AstraZeneca products must report this to Global Security.

    The Company supports supply chain partners in identifying and establishing the controls needed to ensure authenticity of product through the end to end supply chain. The Company does not tolerate unlawful activity and will take appropriate action if a partner is found to be involved in any type of illegal trade as documented in the Counterfeiting Zero Tolerance Standard for Supply Chain Partners.

14. **Security principles.** The Company is committed to creating a secure business environment: protecting patients, staff, products, property and information; minimising losses and disruption; and safeguarding the Company's reputation. Security must be managed as any other critical activity in the proposal, planning, conduct and discontinuation phases of business operations. Line managers are accountable for implementing security controls and processes that meet local needs and the requirements of this Policy and supporting Security Standards. In particular, they must ensure that:

    - Security risks are identified and documented and appropriate measures implemented to manage them;

    - Security risks and mitigation measures are reviewed at least annually, and in the event of any major change in the business or local security conditions;

    - The security implications of all aspects of work carried out by others on behalf of the Company are considered;

    - Security incidents are reported, investigated, recorded and communicated appropriately;

    - Armed security is not used unless it is a legal requirement or there is no acceptable alternative to manage the risk. Any proposals to use armed security must be referred to Global Security for approval.