AstraZeneca

IT Security Policy

Version 14

1. Background, Purpose and Scope

Background

AstraZeneca's (AZ's) information and information systems are an asset of significant value. Disciplined management of information enhances the value, supporting decision-making and operational success and is integral to the way we use it.

The objective of the IT Security Policy is to provide reliable information, data, and computing services within AZ and ensure appropriate controls are in place to protect the confidentiality, integrity, and availability of information.

- **Confidentiality** – Addresses preserving restrictions on information access and disclosure so that access is restricted to only authorised users and services
- **Integrity** – Addresses the concern that sensitive data has not been modified or deleted in an unauthorised and undetected manner
- **Availability** – Addresses ensuring the timely and reliable access to, and use of information.

Purpose

All information and its assets are critical to AZ's operations and provide the ability to achieve the strategic objectives of the organisation. In line with this requirement, the IT Security Policy provides a comprehensive framework for:

- Creating a leading practice Information Security Management System (ISMS)
- Supporting AZ's strategic vision through a risk-based approach which effectively balances usability and security
- Facilitating a 'security aware' culture across AZ and promoting that information security is everyone's responsibility
- Protecting AZ, its employees and patients from illicit use of AZ systems and data
- Ensuring the effectiveness of security controls over data and systems that support AZ's operations
- Recognising the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related cyber security risks
- Providing for the development, review and maintenance of minimum-security controls required to protect AZ's data and systems.

The policy statements set the 'ground rules' under which AZ operates and safeguards its data and systems to both reduce risk and minimise the effect of potential incidents.

The policy statements, including their related control objectives, standards, procedures and baselines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure AZ users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help AZ comply with current and future legal obligations.

Scope

The IT Security Policy applies to all information assets (physical, informational, paper, people, services, site, IOT, firmware, hardware and software), and underlying IT (Information Technology) and OT (Operational Technology) technologies and services (i.e. storage, backup, server hosting services, application services etc) that AZ owns and / or utilises.

These Policies do not supersede any other applicable law or higher-level company directive or existing labour management agreement in effect as of the effective date of this policy.

Audience

The Policies defined in this document apply to all AZ employees using AZ’s information systems and assets.

The Policy shall also be applicable to all external/third party companies/personnel (i.e. vendors, third party resources, consultants, interns/trainees, contractors employed by AZ and clients/ customers visiting AZ offices who engage in work and have access to AZ's information or information processing facilities).

AZ's documented roles and responsibilities provides a detailed description of user roles and responsibilities, regarding cyber security-related use obligations.

Roles and Responsibilities

The Global Head of Cyber Security and the Cyber Security Leadership team shall be responsible for maintenance and accuracy of this policy.

The requirements of this policy and supporting standards are important for the protection of AZ information, IT / OT assets and the delivery of medicines to patients. It is the responsibility of individuals and teams that manage IT / OT solutions to consider cyber security risk and to select and apply the appropriate controls within this document. Functional teams should follow processes to ensure cyber risk and controls are considered throughout the lifecycle of AZ’s IT / OT solutions.

2. Policy Statements

AZ aligns cyber security defences to the globally recognised industry best practice NIST Cyber Security Framework (CSF) which recognises five critical functions:

	NIST CSF Function	Purpose
	IDENTIFY	Develop the organisational understanding to manage cyber security risk to systems, assets, data, and capabilities
	PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
	DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
	RESPOND	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
	RECOVER	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

The following policy statements (by NIST function) must be applied by all employees, but primarily enacted by owners and operators of AZ's IT and Operational Technology (OT) assets. The associated IT SPF Standards documents state the Requirements necessary to comply with these policy statements.

IDENTIFY	**IT ASSET MANAGEMENT** We protect our IT assets by implementing and maintaining appropriate IT Asset Management (ITAM) business practices across AZ. This is to ensure that technology assets are properly managed throughout the lifecycle of the asset, from procurement through to disposal.
	SECURITY GOVERNANCE MANAGEMENT We protect the confidentiality, integrity and availability of our data and systems, regardless of how our data is created, distributed or stored. Digital security controls will be implemented in accordance with all statutory, regulatory and contractual obligations. This is to ensure the development, proactive management and ongoing review of our security and privacy programmes.
	INFORMATION ASSURANCE We carry out due care and due diligence activities throughout an asset's lifecycle by conducting periodic assessments to evaluate the effectiveness of applicable security controls. This is to ensure reasonable assurance is used in the development, implementation, assessment, authorisation and monitoring of the security programme.

IDENTIFY	**RISK MANAGEMENT** We assess and respond to the cyber risks to operations, assets and data which support our business processes and take appropriate action to remediate unacceptable risks. This is to ensure that cyber security risks are visible to and are understood by business units that own assets or processes.
	PROJECT & RESOURCE MANAGEMENT Risk is managed throughout the Secure Development Life Cycle (SDLC). Therefore, all technology projects and programmes address resource requirements to implement and maintain appropriate security controls through the life cycle of the asset(s) or service(s). This is to ensure resource management addresses cybersecurity requirements across project and programme management enterprise-wide, regardless of the type of the project.
	THIRD-PARTY MANAGEMENT We assess the cyber security and privacy risks posed by our third-parties, to ensure that they implement security controls aligned to our needs. This is to ensure that security and privacy risks associated with our third-parties are mitigated or avoided.

PROTECT	**IT CAPACITY PLANNING** To prevent business interruptions, we proactively manage the capacity and performance of our critical technology and supporting infrastructure.
	IT MAINTENANCE The periodic and ongoing maintenance and upgrades of our IT assets, as well as those of our third-parties are performed and governed appropriately, to minimise the risk from evolving threats.
	SECURITY STANDARD FOR IT CHANGE MANAGEMENT Changes to IT assets must follow a standard process to reduce the risk associated with change, establishing appropriate steps in the recording, assessment, authorisation, scheduling, implementation, review and closure of IT changes
	ARTIFICIAL INTELLIGENCE (AI) & MACHINE LEARNING (ML) AZ develops and implements trustworthy and resilient ML models that utilise AI in a beneficial manner to the organisation.
	CLOUD COMPUTING We proactively manage risk in our private and public cloud environments through secure architectural decisions and implementations that keep the environments secure and efficient.
	SECURE CONFIGURATION MANAGEMENT We maintain accurate inventories of our technology platforms and enforce security configuration settings to protect the confidentiality, integrity and availability of our systems.
	CRYPTOGRAPHY AND KEY MANAGEMENT Appropriate cryptographic safeguards are used to protect our Strictly Confidential and Company Restricted information against loss, unauthorised access or disclosure, when both at rest or in transit. This is to ensure the confidentiality and integrity of our data.

PROTECT	**INFORMATION CLASSIFICATION** We protect our data by applying data classification, limiting access to authorised users and utilising methods of sanitising or destroying media so that data recovery is technically infeasible. This is to protect our data from unauthorised disclosure and meet regulatory requirements.
	INFORMATION LABELLING AND HANDLING We protect data in both hardcopy and digital form by limiting access to authorised users and utilise methods of sanitising or destroying media so that data recovery is technically infeasible.
	EMBEDDED TECHNOLOGIES We address the security risks associated with types of embedded operational technology (Internet of Things, Industrial Controllers/Devices etc), to prevent risks to our partners, patients and employees.
	CORPORATE IT USAGE We ensure standardised, documented practices are followed by employees when operating, or interacting with AstraZeneca IT assets in the course of their roles.
	HUMAN RESOURCES SECURITY We apply cyber security practices to our human resources processes to foster a security culture, supporting innovation and scientific leadership.
	IDENTITY AND ACCESS MANAGEMENT We implement the principle of “least privilege” across our logical access control mechanisms so that only authenticated and authorised users can gain access to our systems and data, in an accountable manner.
	MOBILE DEVICE MANAGEMENT We apply security controls to govern the use of our mobile assets, including third-parties, to ensure our employees can collaborate securely.
	NETWORK SECURITY We implement the concept of “least functionality” for our network infrastructure and deploy security mechanisms to keep our networks secure from evolving threats. We provide situational awareness of network activity so that proactive measures can be implemented to address evolving threats.
	WEB SECURITY We implement the principles of “least privilege” to reduce risks associated with managing internet-accessible technologies and we ensure that security and privacy controls are in place to satisfy applicable statutory, regulatory and contractual requirements.
	PHYSICAL SECURITY & ENVIRONMENTAL MANAGEMENT FOR AZ–OWNED ROOMS We implement appropriate controls to limit physical access to our systems and equipment to only authorised and appropriate individuals. Where we host critical IT systems, we operate appropriate environmental controls to ensure the correct conditions exist to avoid preventable hardware failures and service interruptions.
	IT PRIVACY BY DESIGN We align with privacy principles and implement appropriate security controls to protect the Personal Data and Sensitive Personal Data that we are entrusted to process, store and transmit, to protect against inappropriate use, or loss.

PROTECT	**SECURE ENGINEERING AND ARCHITECTURE** Our cyber security architecture supports our technology architectural direction and business strategy. Our secure engineering principles address applicable statutory, regulatory and contractual obligations to implement and manage reasonable security measures, as defined by industry recognised leading practices.
	SECURITY AWARENESS AND TRAINING We ensure our employees are aware of the cyber security risks facing the company and our people and that they adopt and implement the appropriate behaviours needed to mitigate or remove any risk from these.
	TECHNOLOGY DEVELOPMENT AND ACQUISITION We implement the principles of “least privilege” and “least functionality” when developing and/or acquiring new technology. This includes the deployment of adequate security measures during the technology’s life cycle to ensure security and privacy risks are identified and appropriately remediated at all stages.
	ENDPOINT SECURITY We implement the concept of “least functionality” for our technology endpoint devices and proactively govern security mechanisms to keep them secure from evolving threats.

DETECT	**THREAT INTELLIGENCE MANAGEMENT** We maintain the capability to proactively govern threats, including the identification, assessment and remediation of threats to our systems, data and business processes.
	CONTINUOUS MONITORING AND SECURITY OPERATIONS We maintain a continuous central logging and monitoring capability to provide early awareness of cyber security events. This is to provide situational awareness, to enable fast response to mitigate risk and to minimise the potential for further cyber security incidents. We maintain an effective security organisation to provide protective, detective and response services to meet the requirements of the business. This is to ensure security functions can be effectively carried out across the organisation.
	VULNERABILITY & PATCH MANAGEMENT We proactively manage cyber threats across the AZ estate via a risk-based approach, primarily focusing on risks presented to the business from vulnerabilities or misconfigurations that are being actively exploited.

RESPOND	**BUSINESS CONTINUITY** We establish and manage the capability for maintaining continuity of business to ensure the availability of critical technology resources during adverse conditions.

	CYBER SECURITY INCIDENT MANAGEMENT We maintain a cyber security incident handling capability that includes adequate preparation, detection, analysis, containment, recovery and reporting activities. This is to guide AZ's response when security incidents occur.

RECOVER	**IT DISASTER RECOVERY** We establish and manage the technical capability for maintaining the Continuity of Operations (COOP) to ensure the availability of critical resources during adverse conditions.

N.B AZ reserves the right to revoke, change or supplement these Policies at any time without prior notice. Such changes shall be effective immediately upon approval by management unless otherwise stated.