AstraZeneca

Owner
Smoley, David

Authors
Buckwalter, Peter (MedImmune)

Approvals

Approval Reason	Approver	Date
Reviewer Approval	Buckwalter, Peter (MedImmune)	2015/03/26 16:42:49

ASTRAZENECA GLOBAL POLICY

CORPORATE INFORMATION TECHNOLOGY USAGE POLICY

1. PURPOSE

This Global Policy sets out the requirements for ensuring the appropriate use of information technology ("technology") across AstraZeneca.

2. AUDIENCE

This Policy applies to all Employees.

Other Third Parties who use technology to perform or deliver services for, or on behalf of, the Company are expected to follow standards consistent with the principles of this Policy.

3. SCOPE

This Policy represents the minimum company requirements related to the use of technology to conduct company business. Where local laws and regulations are more restrictive than this Policy, the more restrictive rules must be followed.

For the purposes of this policy technology includes all computer devices including mobile devices, computer networks, computer and information management services including cloud services, system software and application software

Through collaborations with private, public and academic organisations, AstraZeneca shares, uses and manages information and technology assets that belong to organisations other than AstraZeneca. The principles in this Policy apply to the use of technology, regardless of its ownership, used to perform or deliver services for or on behalf of the Company..

4. POLICY STATEMENTS

4.1 Principles

AstraZeneca's technology is provided for business purposes. AstraZeneca permits limited personal use provided;

- It is not contrary to the interests of AstraZeneca or to local policy,
- It has no adverse effect on job performance or on IT operations.

The Company will not accept liability for the outcome of any personal transactions. Examples of personal use that is not permitted include;

- Running non-Company businesses,
- Creating or operating non-Company Internet sites,

- Excessive use of devices (e.g. phones) or services (e.g., the Internet). Costs associated with excessive use are the responsibility of the individual

AstraZeneca may access personal activity and content in exceptional circumstances and in accordance with the requirements of local laws.

You must comply with the principles set out in the AstraZeneca Code of Conduct. The following are examples of activities which are not acceptable:

- Viewing or handling offensive, obscene or unlawful material or any content that might compromise the Company's reputation,
- Gambling through the use of company devices,
- Using devices (e.g., network monitors, network scanners) or services that are not authorised for company use, as described in the policies and standards the Company sets,
- Using or altering devices, services, networks, system or Application Software to disrupt or interfere with the normal functioning of services or systems.

The Company may block access to selected Internet sites at its discretion.

4.2 Protecting Information and Assets

Those responsible for the introduction or any part of the lifecycle of IT services and systems must have them evaluated for their impact upon our obligations to patients and business objectives. They must ensure compliance with this and other IT policies and standards the Company sets.

You must protect Company Information from threats. You must take reasonable precautions to prevent malicious software from entering devices, software, services, and networks used to access Company Information. If you are suspicious, you must not open or download email, files, attachments or links.

You must not use the computers provided in public places, such as those in Internet cafes, airport lounges and at conferences to access company systems or information described as Personal Data or Sensitive Company Information.

You must take reasonable precautions to prevent unauthorized viewing of Company Information while you are in public spaces.

You must store and retain Company Information in a manner that complies with the GRAD schedule and any Legal or eDiscovery requirements

You must only use the methods authorised for company use, as described in the policies and standards the Company sets, to access networks, access information, protect information and transmit information. You must protect Sensitive Company Information during its transmission so that it cannot be accessed or understood by unauthorized persons. You must encrypt Personal Data during its transmission over the internet.

At all times, you must protect Sensitive Company Information. This includes prohibition against sending such information via email, cc, forward or auto-forward to accounts not controlled or managed by AstraZeneca or its partners, or otherwise using insecure file storage services or systems. If in doubt, consult the policies and standards the Company sets on information

management and information classification for advice about appropriate protection measures authorised for company use.

You must ensure that any use of removable media or portable storage devices is compliant with applicable legal or regulatory (e.g., Data Protection, copyright, export control) requirements.

You must only use removable media or portable storage devices for Personal Data if the data is encrypted.

You must only connect removable media or portable storage devices (e.g., memory cards, USB drives) containing Sensitive Company Information, to devices, systems or networks that are controlled or managed by AstraZeneca or its partners.

You must report suspicious events, such as possible virus infections, unauthorized use of accounts, tampering with, or disruptions of company services to your IT Service Desk immediately and follow their instructions.

You must protect equipment against loss, damage or theft. In the event equipment is lost or stolen you must inform your line manager and IT Service Desk immediately. If the theft occurs outside of company property, you must also inform the proper law enforcement authorities.

4.3 Protecting Access

You must secure your passwords and protect your corporate identity from theft and unauthorized use. You must not share company passwords with anyone.

You must only access Company Information or systems required to perform your assigned responsibilities.

You must prevent unauthorized access to company software, services, networks or information. Individuals that approve access to Company Information must only grant privileges to those they know require it for specified business purposes and only for the specified time needed to perform assigned responsibilities.

4.4 Collaborating Securely

You must only share Company Information with persons who have been granted permission and have a business need. You must only share it for the specified time needed to perform assigned responsibilities.

You must store Company Information in secured (e.g., password or access key protected) storage places which restrict access to authorized users. Personal Data must be encrypted when stored on Internet/cloud based collaboration tools.

4.5 Personal Devices

The Company permits employees to use personally owned devices to access specific business systems and services. You must not use a personally owned device to access business systems and services except where such access is expressly permitted for the purpose you intend. In particular, you may not download Strictly Confidential data to the device (including capturing

screenshots) unless permitted. Use of personal devices is subject to the full provisions of this Policy and may also be subject to other AstraZeneca policies, standards and procedures.

AstraZeneca reserves the right to erase or remotely wipe data from any personally owned device where AZ data is being held. While the erasure process will targets AZ data wherever possible it may also affect, personal data, apps and settings on your device.

You should secure your device and Company data against loss, theft and use by unauthorised persons. This includes protecting your device with a pin or strong password, keeping it current with security patches and updates and not downloading or installing untrusted software or applications. Where possible you should avoid inclusion of company data in device backups. Backups of your device must be encrypted.

Use of a personally owned device to access business systems is at your own risk and AstraZeneca shall not be responsible for any loss, damage or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to the device, it software or functionality.

AstraZeneca may require you to give access to a personally owned device in circumstances where there is a requirement to retrieve corporate data for legal purposes.

4.6 Acceptable Use

Software developed by, for or on behalf of AstraZeneca is the property of either AstraZeneca or a contracted business partner. You must only use it for its intended business purpose.

To ensure compliance with legal requirements;

- All computer devices, computer services, computer network, software and electronic material (e.g., publications, recordings) use must comply with applicable licenses, notices, contracts, agreements, regulations and import and export control laws,
- All software used to conduct AstraZeneca business must be properly licensed for its intended business purpose,
- Licensed or purchased software must not to be copied without the correct license to do so.

Failure to comply with this Policy, its supporting policies, or the laws and regulations of the countries in which you work will be fully investigated and corrective action may be taken, up to and including termination of employment, depending on the circumstances. Violation of law can also result in imposition of criminal or civil fines and other penalties depending on applicable law.

5. GLOSSARY

Terms	Definition
Application Software	Software programs, designed for end users, that run on computing devices

Company Information	Information that the company or trusted partner creates, uses or handles, in all formats including physical, electronic or verbal, or the use of other knowledge in the course of Company business (For further information consult - Information Classification Standard)
Cloud Services	Computer and information services provided, hosted and operated by third parties.
Encryption	The process of protecting a message so that it can be read only by the sender and the intended recipient. This is accomplished through use of products such as PGP, BitLocker, Pointsec and WinZip.
GRAD	The Global Retention and Disposal (GRAD) schedule, provides a complete list of all AZ business essential records with information on how long each record should be kept (retention) for business, regulatory and legal purposes. Compliance with the GRAD Schedule is mandatory.
IT	A generic term to include all aspects of computerised systems and their management, from application to infrastructure, both hardware and software, whether for information management or control purposes
Network	A system of interconnected electronic components (e.g. computing devices, hard drives, printers, routers, switches) and circuits linked together so that they can communicate, exchange commands and share data, hardware and other resources. Examples of networks include the AZ corporate network, the Internet, and external service provider networks
Personal Data	Any information about an identified or identifiable natural person (For further information consult - Code of Conduct)
Sensitive Company Information	The following gives an examples of the types of information that constitute sensitive information

6. REVISION HISTORY

Version	Description of Change
1.0	This Policy replaces the Computer Usage Policy.
2.0	Updated the Personal Devices section