AstraZeneca

Owner	Authors
Askem, Ian M	Ambrose, Peter

Approvals

Approval Reason	Approver	Date
Quality Approval	Leonard, Sara E	2018/12/10 16:08:39
Owner Approval	Askem, Ian M	2018/12/12 16:01:02

ASTRAZENECA GLOBAL STANDARD OPERATING PROCEDURE

USAGE OF 3RD PARTY DEVICES IN SEGREGATED NETWORKS

1. PURPOSE

This is the process that needs to be followed for any vendor/contractor Laptops, removable storage devices and any new equipment/servers from outside of AZ, before they connect their devices to AZ Segregated Network

2. AUDIENCE

The following areas are involved in managing the Infrastructure and have roles and responsibilities, defined within this document.

- CSIS – Cyber Security and Infrastructure Services
- Operations IT
- Local Site Operations (Ops) (for example – Engineering)
- ASK IT/ Desktop support team

3. SCOPE

The scope of this SOP covers the processes for third party (non-AZ) devices that needs to be connected to a segregated network for any support or troubleshooting purposes. This includes vendor laptops, USB storage devices along with the usage of guest wireless or 3rd party internet using mobile (4G/5G) services with in Segregated Networks.

4. PROCEDURE

Only approved vendor/consultancy with a maintenance/support contract with AZ is allowed to connect to AZ segregated networks. To protect AZ devices from any virus attack or any vulnerabilities, vendor devices like memory sticks and laptops must be assessed for threats before connecting to the manufacturing network or any equipment in the manufacturing area. The following sections covers the procedure that must be followed before connecting a 3rd party device to AZ Segregated network.

4.1 Requirements for a non-AZ laptop to access segregated network

Vendor/Consultant:

1. Inform the host department that Vendor(s) have arrived at the site and want to connect to equipment that is on the segregated network
2. Approval is required from the owner of the Bronze network locally to attach any Non-AZ computing devices into Bronze network. In the event, if a dedicated IP Address is required, one will be assigned by the Ops team with the approval from the site responsible person.
3. The following needs to be up-to-date on the vendor device and should be evidenced to an appropriately competent person.
    a. Microsoft Security patches
    b. Antivirus version
    c. Antivirus signature file

Segregated Network Management and Support Team:

1. Confirm that the Operating System Security patch level is up to date on the Vendor laptop.
2. Verify that current reputable anti-virus software is installed on the vendor laptop. If unsure consult with the SOC team.

Exceptions to these steps are at the digression of the owner of the Bronze network locally.

4.2 Requirements for connecting a USB Storage device to the segregated network

Given the material cyber security risks when using USB storage devices, their use should be avoided wherever possible. (e.g. by utilising file transfer via Gold zone hosted fileshares etc.). Where their use is unavoidable the following principles should be applied:

a) the USB storage device should be inserted into an AZ laptop or computer that has the latest corporate AV scanning software installed, and a full scan of the device should be performed by an appropriately competent person (e.g. an IT experienced end user, or local IT support professional), to ensure the correct completion of the scan, and appropriate evaluation of the results of the scan
b) even with a full scan, there remains a residual risk of infection. However small, that residual risk should be consciously accepted by the appropriate system owner

c) individuals should contact the SOC team if they need further information, advice or guidance regarding the cyber security risks associated USB Storage devices in Segregated Networks.

4.3 Vendor Use of Guest Wireless and 4/5G Mobile Data Service in Manufacturing Network

The use of Guest Wireless and 4/5G Mobile Data Services in Manufacturing Networks is permitted only in exceptional circumstances and at the discretion of the owner of the Bronze network locally and on devices that have met the criteria outlined in section 4.1 above.

The following procedural steps must also be followed:

4.3.1 Procedure

If a vendor uses any of the following;

- AZ-Medi-Guest WIFI services
- 3g/4g/5g services via a SIM card in his laptop
- Any tethering arrangement via a cellular phone or dedicated device to access
- Google Mail, Hotmail or any other Webmail services
- Any social media (Facebook, Twitter etc)
- Any other website, including his own corporate remote access facilities

Then at the time of access, the vendor's device must NOT be connected to any AstraZeneca Computing Device by TCP/IP connection, USB connection, File share or any other way that may allow malware to traverse from the external network to the AstraZeneca Network.

5. RESPONSIBILITIES

Roles and responsibilities provide a clear understanding of whom and what activity each person involved in providing support for network segregation services should play. Each RACI matrix identifies the team or teams Responsible, Accountable, Consulted, Informed and a definition of the meaning of each is provided below.

Relationship	Letter	Definition
Responsible	R	The “doer” consists of the team(s) who complete the task or a participant in the completion of the task. The “doer” is responsible for the action/implementation. Responsibility can be shared.
Accountable	A	Designates the individual or team that is ultimately answerable for an activity or decision. Has oversight, governance and accountability for the performance of actions related to the task.
Consulted	C	Consulted identifies the team or team(s), typically subject matter experts, to be consulted as part of the action or final decision.
Informed	I	Informed identifies the individuals who need to be informed after a decision or action is taken. They may be required to act because of the outcome. It is one way communication.

Table 1: RACI Definitions

Roles	Key Responsibilities
Site Responsible Person	Management Approval Ensuring that suppliers are aware of these requirements
Vendor/Consultant	Obtain approval from Site Responsible Person and inform concerned host department when the Vendor is on site.
Process Control Engineer	Verify and confirm vendor device is compliant and ensure that the vendor complies with the responsibilities detailed.

Table 2: Roles and Responsibilities

Below table provides the RACI summary for the activities covered in this SOP.

Activity	Site Responsible Person	Ask IT / Desktop Support	Ops IT	Local Site Operations	Vendor
Connecting the laptop to network & IP address allocation	C	-	-	RA	C

Activity	Site Responsible Person	Ask IT / Desktop Support	Ops IT	Local Site Operations	Vendor
Approval for External device for use on AZ network	A	-	-	R	-
Ensure Vendor device has current, reputable AV software installed				AR	I

Table 3: RACI Summary of Activities

6. GLOSSARY

Terms	Definition
AZ	AstraZeneca
AD	Active Directory
Zone	A part of a Network that is defined by a discrete set of addresses and corresponds to an IP subnet
CSIS	Cyber Security & Infrastructure Services
PCN	Process Control Network - A computer network that has been isolated from AstraZeneca Corporate network by means of buffer devices
LAN	Local Area Network
Segregated Network	A computer network that has been isolated from AstraZeneca Corporate network by means of buffer devices
PCE	Process Control Engineer who manages the Segregated Network and is part of the Ops team
AV	Anti-Virus software
RDF	Remote Desktop Terminals
SEPM	Symantec Endpoint Protection
GUP	Group Update Provider
CMMS	Computerized Maintenance Management System

7. REFERENCES

The following corporate standards and procedures must be complied with. This SOP provides practical guidance on how to comply with these standards.

#	Document Name	Reference ID	Embedded Document/Reference Link
01	ITSEC - Network Isolation Guideline - AZDoc0029541	AZDoc0029541	Network Isolation Guideline
02	AZ ownership and management of segregated networks Standard	TBC	AZ ownership and management of segregated networks Standard
03	Inventory Management in Segregated Networks	TBC	Inventory Management in Segregated Networks

8. REVISION HISTORY

Version	Description of Change
1.0	New Document
1.1	Redraft based on site inputs and consultation with SOC
2.0	Updated as per comments from SOC team

9. APPENDICES

N/A