SOP for Network Policies

Avanza Network Policies & Procedures

October 15, 2020

Version: 3.0

Document Information

Document title:	SOP for Network Policies
Document file name:	Network Policies & Procedures
Issued by:	Aibad Ahmed Siddiqui
Issue Date:	15th October 2020
Reviewed By:	

Table of Contents

1 Purpose

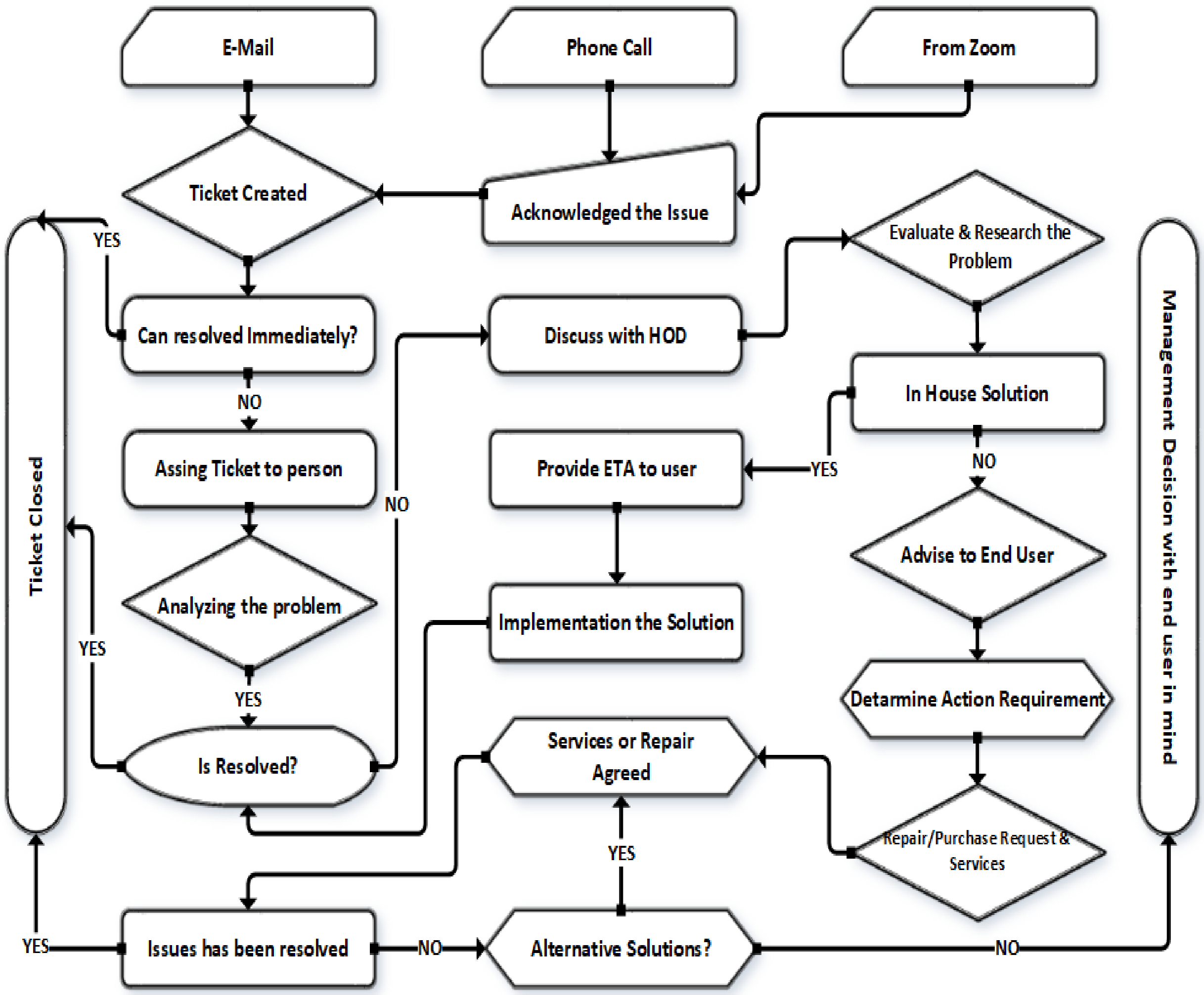
The purpose of this document is to have Information Systems [IS] Department's Operational Policies & Procedure defined and practiced accordingly so that the results are consistent & predictable.

2 Scope

This document covers the following aspects of Data and network:

- IS Work Flow
- IS Security
- Biometric Registration
- Antivirus
- Password Maintenance
- User Data Backup
- Code Repository Access
- Database Access and Protocols
- Take IT Equipment On-Site
- Video Conferencing
- Email
- Server Backup and Restoration
- Printer
- Servers
- Inventory
- Hardware and Software Maintenance
- Hardware Supplies & Repairs
- IP PABX
- Use of Internet
- VPN
- Network, Mobile Phone & Internet Connections
- General Misuse

2.1 IS Workflow



2.2 IS Security

- The IS department will provide each member of Avanza a Domain username and password, which is required in order to gain access to computer.

2.3 Biometric Registration

As per HR, all Avanza employees are to be registered with Biometric Attendance System which will then be incorporated in HRMS. I.S maintains new & existing users on the Biometric system along with Registration for New Joiners.

2.4 Antivirus

- Antivirus Software with Real time Protection is installed on all the Desktops, Laptops and Servers in order to protect these machines from known/unknown threats including viruses, Trojan and Network Based Attacks.
- End-user is responsible to timely update the virus definitions from Internet and protect their systems at all cost.
- I.S will monitor and update all existing /future servers with Antivirus Definitions.

2.5 Password Maintenance

- The password for all critical servers, Firewall, Switches/Routers and Avanza FTP Server is set. *(Administrator/provided user Password never change without Intimation of I.S Team)*
- *Passwords have managed over password Manager tool*.
- The Unit Head is intimated about the password change and the process is ended
- Users can only set their password that includes special characters, alphanumeric values and minimum length is 12 characters.
- Users must be changing their password within 60 days (No Previous passwords will be used)
- Don’t share your password to anyone.

2.6 User Data Backup

- IS don’t take any types of User/Client data backup even if it’s stored and saved on Shared Folders on Server.
- All SE, SSE, DM are required to save Software Codes/Patches/Files in their

respective repositories on SVN, Gitlab etc. on daily basis before leaving office.

- In case of Disaster or User System/Laptop crash IS will not be responsible for any Data Loss.
- All previous Email Files Backup are the responsibilities of End-User.
- *If Required I.S can run Data Recovery software but there is no chance that your data is fully/partially recovered.*
- In order to safely recover from unavoidable conditions like Theft/Snatching, all your important Data/Files are to be stored in a safe location

2.7 Code Repository Access

- I.S will assign rights (read/write) to the repository over Gitlab/SVN. Users should include their DMs in same Email.
- IS will revoke rights from the repository upon request.
- Users can access repository URLs by using their Domain ID and password.

2.8 Database Access and Protocols

- Access to the databases hosted on servers in premises would be possible via User ID and password provided by I.S.
- Users could initiate requests to access any database by mentioning its complete name, Server Name/Version/IP. This access request should include DMs in Email. Then, access to that specific database would be provided by IS.
- Request of importing databases would only be entertained if backup is provided along with its log file.
- I.S will not restore any database which contains any sensitive client data.
- Users should make sure the database they have received from the client should not have any critical client data.
- It is the responsibility of the user to verify that the database does not contain any sensitive client data, prior restoring databases locally.

2.9 IT Equipment Onsite

- Any Desktop, Laptop, Printer, Portable USB Drive, USB Flash Drive provided by the Avanza is subject to the same conditions of use whether used at home or in the office.
- Users should take all reasonable care and precautions to ensure safe transport and storage when moving equipment between home or other remote locations and work.
- Users are responsible for data confidentiality.

2.10 Video Conferencing

Video Conferencing facility is available in the meeting rooms which can be utilized for official purposes as and when required and on the availability of meeting room.

2.11 Email

Email services has been managed by I.S Team it is hosted in Microsoft 365.

2.12 Server Backup and Restoration

Three types of backups are managed by I.S department.

a) Critical backup (All mission critical servers' backup on daily basis)

b) Weekly backup (This is scheduled backup)

c) One Time backup (This type of backup is only taken by user request)

I.S team also managed D.R sites that contains all mission critical server live Syncing

2.13 Printers

- Printers are allocated throughout the premises to facilitate all Units who have a legitimate necessity of it. In order to provide unprecedented access of printers IS has incorporated Network printers. Every user is given the printer access as per his/her needs.

- IS also maintains comprehensive logs of print jobs and transactions sent by any user, or the number of jobs being printed on any network printer in order to keep the evidence and control the misuse of printers.

Note: Don't print papers until it is extremely necessary

2.14 Servers

Department wise list of servers are maintained. If a server is required by an employee, then his Unit Head will send a formal request to the IS department via VM request form. After the end date which is provided in VM request form I.S will be shutoff your VM without intimation.

2.15 Inventory/Hardware request.

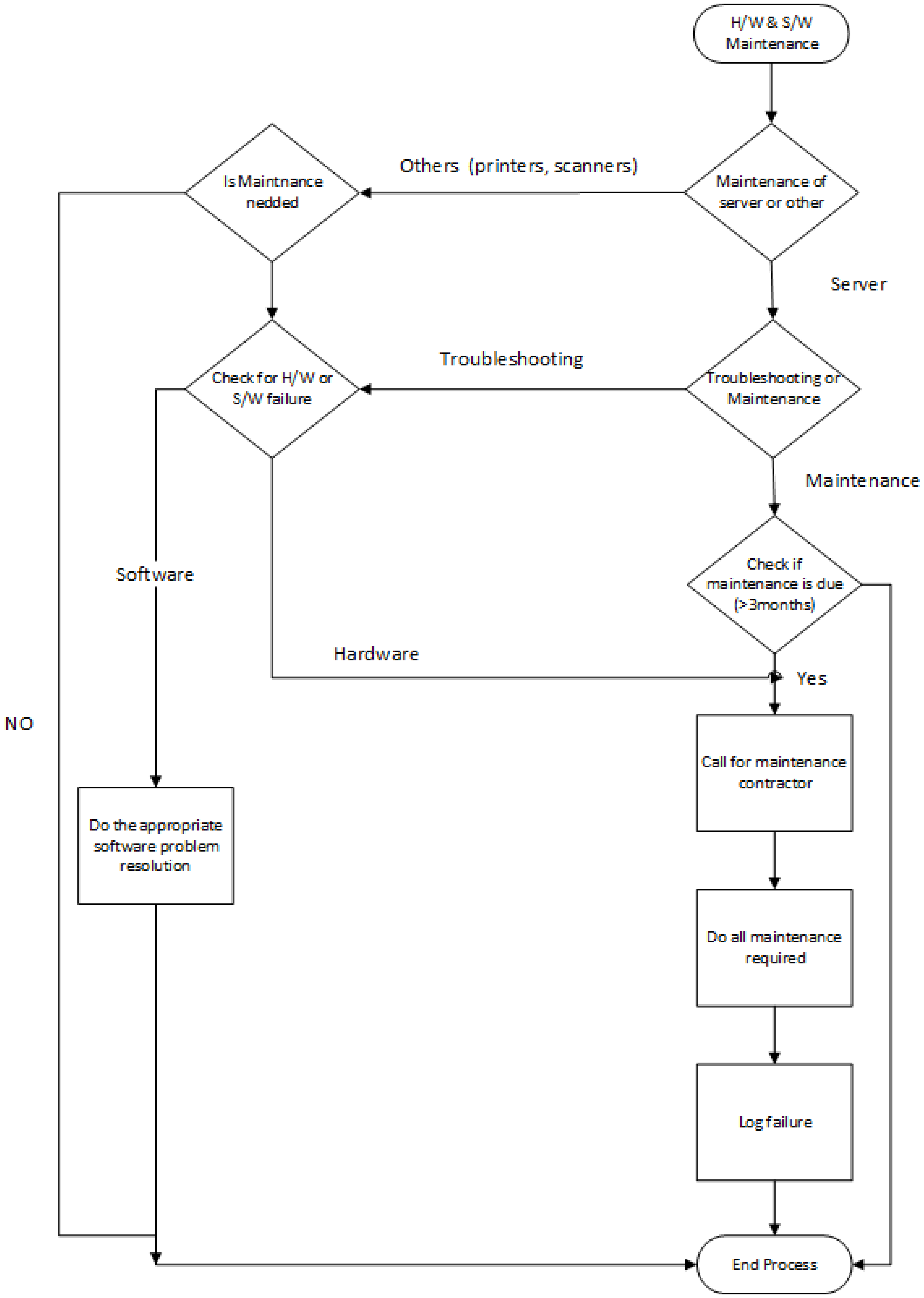
Inventory or computer related hardware is maintained on a day-to-day basis. When the inventory level reaches to zero a requisition is submitted to the admin department to refill inventory.

2.16 Hardware and Software Maintenance

- At first analysis will determine if the maintenance is required for servers/workstation or other peripheral devices.

- If peripheral devices requires maintenance (printer, scanner, CD writers) instead of the server, it is determined whether maintenance is needed or not. If it is not, the process is ended. If maintenance is needed, go to point 8.
- If maintenance is to be done for the server, it is determined whether troubleshooting or maintenance of the server is required.
- If troubleshooting is required for the server, go to point 8.
- If maintenance is required, it is checked whether maintenance is due, that is, if it has been over three months since the last maintenance was performed.
- If maintenance is not due, the process is ended.
- If the maintenance is due, maintenance contractor is called. Go to point 11.
- In case troubleshooting of the server is required or if maintenance of other machines is needed, it is checked whether there is a hardware or software failure.
- If there is a software failure, the appropriate software problem resolution is performed and the process is ended
- If there is a hardware failure, the maintenance contractor is called.
- All maintenance required is performed and the log for the failure is entered. The process is ended.

2.16.1 Flow Chart


H/W & S/W Maintenance
Maintenance of server or other
Others (printers, scanners)
Is Maintnance nedded
Server
Check for H/W or S/W failure
Troubleshooting
Troubleshooting or Maintenance
Maintenance
Check if maintenance is due (>3months)
Software
Hardware
Yes
NO
Call for maintenance contractor
Do the appropriate software problem resolution
Do all maintenance required
Log failure
End Process

2.16.2 Equipment Movement

No equipment should be moved or swapped between staff without first informing the IS Department.

2.16.3 Disposal of Equipment

Legacy IT equipment should not be disposed of by anyone other than the IS & Admin department who will arrange for disposal in accordance with the Company Policy.

2.17 Hardware supplies and Repairs

- For the prevention of the Hardware equipment, all hardware equipment will be serviced on as-is basis by the Desktop Engineer. The IS Engineer will also make sure the equipment is placed in a climate recommended by the technical specification of the equipment.
- All consumable items Keyboard, Mouse, Charger, Laptop Battery, and Headset are provided only after thoroughly checking of the faulty item. The requirement will be cross-checked with the last installed one before a replacement is provided
- Hard Disks, RAM, Desktop Power Supplies are replaced with faulty ones from IS existing pool. However, if the replacement is not available within IS, same will be procured within 5 days as per Avanza Procurement Policy.
- Every new Laptop is provided with standard Laptop Bag
- It is the responsibility of every user to properly Charge and discharge laptops batteries to avoid abuse of office supplies. Laptops should be charged with Original Charger/A Grade Charger only.
- Desktops / Laptops are assigned to resources on Permanent and on-site travelling basis, proper safety and handling during office and non-office hours are the responsibility of end-user.
- Use of Projector, Video Conferencing and IP Phones are expensive piece of equipment. Please handle it with care. These services will not be used for personal usage.
- IS will upgrade all the Laptops/Desktops to a standard configuration approved by Management
- Report any equipment malfunction or problems to IS

2.18 IPPABX

- IP PABX is managed by IS. Assigning of Extensions on Soft Phone, Analog Phone, and IP Phones will be provided as per the company policy.
- International Dialing is only available through Operator.
- Mobile/Local dialing options are available from all the phones.
- Fair usage is the responsibility of all the users, otherwise the management reserves the right to charge from user.

2.19 Use of Internet

- Access to the internet is primarily provided for work related purposes. That is for Avanza work or for professional development and training.
- Internet use takes up capacity on our network. Use of Internet for personal purposes is prohibited. Avanzian must act in accordance with their manager's local guidelines. The management has the final decision on deciding what constitutes excessive use.
- The IS department have the right to withdraw internet access from any user and globally ban access to any site as appropriate without warning.
- Avanza Solutions will not accept liability for personal legal action (e.g. libel) resulting from staff misuse of the internet.
- Access to social media, streaming websites will be restricted as necessary by IS Department to ensure efficient use of Bandwidth
- The use of the Internet is a privileged facility, not a right. Inappropriate use, including access or download from Internet sites that hold offensive material. Offensive material includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. This list is not exhaustive. Other than instances that demand criminal prosecution, the Management is the final arbiter on what is or is not offensive material, or what is or is not permissible access to the Internet.

2.20 VPN

Associated Document: NW-VPN

2.21 Network, Mobile phone and Internet

Do not connect any device (PC, Laptop, Printer, and Mobile & USB Internet Devices) to the Avanza's data network unless:

- The device is owned by the Avanza Solutions and

- Users could initiate requests to access any database by mentioning its complete name, Server Name/Version/IP. This access request should include DMs in Email. Then, access to that specific database would be provided by IS.
-
- The connection has been approved and set-up by the IS Department.

2.22 General Misuse

- Avanza equipment must not be used for the creation, transmission or deliberate reception of any images, data or other material which is designed or likely to cause offence or needless anxiety, or is abusive, sexist, racist, defamatory, obscene or indecent.
- When communicating electronically, staff is expected to conduct themselves in an honest, courteous and professional manner.
- Any user being aware of, or suspecting, a security breach must immediately alert the MIS Department who will initiate investigation procedures
- Deliberate activities with any of the following consequences (or potential consequences) are prohibited:
  1. Corrupting or destroying other users' data
  2. Tempering of computer hardware including marking / sticking on CPU / Monitor / Keyboard / Printer.
  3. Using equipment in a way that denies service to others (e.g. overloading the network)

********************** End of the Document ***********************

For Further Inquiries

is@avanzasolutions.com | www.avanzasolutions.com