ADIB – Standard

(UAE)

Server Security Standard

STD-ITD-517

Date: 30th May 2023

Version: 6.0

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
6.0	May 2023	All Servers must be ob-boarded through PAM	Alignment with the current practice.
5.0	30th May 2022	Updated ownership to Head of Technology GRC	Alignment with policy.
4.1	30th May, 2021	Document reviewed; no change required.	Process annual review
4.0	Publishing Date	Added controls related to Antimalware/Spyware and PAM onboarding.	To strengthening the security of privileged accounts
3.0	Publishing Date	Added Whitelisted server software list	ITD Process Improvement
2.0	Publishing Date	Converted into new format	ITD Process Improvement
1.3	Publishing Date	NESA Security Control update	NESA Compliance
1.2	Publishing Date	Conversion of the document to new approved STD template	New approved STD template being practiced

Prepared by	Approved by	Reviewed by
IT Governance Team	Head of GRC	IT Governance Manager Head of ITCSA

Document Contents

1 Overview

The objective of this document is to define specification for information security controls of a server installed in ADIB network.

2 Applicability

This standard is applicable to ADIB ITD environment.

3 Standard Owner

Head of Technology GRC

4 Standard Statements

- Server should be located in data center (On-Prem or AZURE CLOUD).
- Server configuration shall be recorded for each individual machine in detail (Serial Number, Server Name, IP Address, Subnet Mask, Default Gateway, Server Type(Virtual Machine or Standalone), VM version, Model, Series, CPU, Memory, Hard Disk, Redundant Array of Independent Disks (RAID) level, Operating System / Service pack / Patch version, Cluster IP, Name and Service Account, Vendor details etc.).
- Server hardware shall be checked for proper installation of cooling fans, power supplies, Network Interface Card (NICs), Peripheral Component Interconnect (PCI) cards, USB , etc.
- Server shall be connected only to local network through wired cable. Other network connectivity options shall be disabled / uninstalled such as Wireless, Bluetooth, Wi-Fi, etc.
- Latest firmware updates, service pack, post-service pack patches, support tools (vendor supplied CD) shall be used and installed by authorized administrator.
- Original copy of every installed software, along-with its previous versions would be maintained, along-with required information and parameters, procedures, configuration details, and supporting software. Audit trail shall be maintained for the installed software, service packs / security patches installed.
- Approved software to be installed, ref. TML-ITD-091 Server Software Whitelist, any exceptions will need to be approved by following the Change Management Process and would be installed by authorized administrators only.
- Whitelisted server software list would be refreshed annually by IT GRC designate.
- Rollback of any software, firmware, security / service pack updates on the server would be maintained, as per the change management process.
- Vendor supported version of application software would only be maintained. Any upgrade in version would be considered as per business need, following the change management practices.
- Changes to servers should follow change management process. Further it should be tested on an identified test / development environment before applying to the production environment.
- Default passwords shall be changed.
- A complex local administrator / root account password shall be set as per the ADIB latest Password Policy.
- The passwords shall be encrypted.
- Unnecessary user accounts shall be removed/ disabled.
- Remote Administration tools access shall be available only to authorized administrator.
- Administrator privilege user activity logging shall be enabled.
- File System Access shall be set for least privileges and enhanced if needed.
- Unnecessary services, shares, file system permission, shall be disabled.
- Services using simple text for authentication shall be disabled.

- Default SNMP Community names shall be changed. The SNMP community shall be accessed only through the designated SNMP server.
- Allow SNMP to be accessed only from local host and SNMP server
- Server shall be running only TCP/IP, with a static IP address, in the proper VLAN.
- Registry entries shall be set for TCP/IP parameters to take care of network/ Denial of Service (DoS) attacks and also for other non-TCP/IP specific parameters.
- Custom banner announcing "Authorized Use Only" shall be created.
- USB shall be disabled.
- All external storage devices (such as USB) shall be disabled, unless authorized otherwise. For the authorized ones, ITD should scan the removable media for malware every time it is connected to ADIB's IT environment.
- Server name shall not include IP address / name of the employee. In case of servers hosted in DMZ, server names shall be unrelated to the application hosted. Every application service user shall use the DNS alias instead of the Server name or IP, unless authorized otherwise.
- Server performance shall be monitored for CPU usage, Hard Disk capacity etc.
- Baseline security shall be implemented on all servers according to functionality.
- Latest Version for Anti Malware/Spyware shall be installed on new servers prior releasing it on Production.
- All Servers must be onboarded through PAM for Remote administration.

5 Exceptions

Any exceptions or exclusion to this Standard requires permission from the Standard Owner.
Any non-compliance to this Standard shall be considered for corrective actions and corresponding corrective action / exception has to be maintained by the Standard owner.

6 Appendixes

Annex I: Acronyms

Acronym	Explanation (Expanded Term)
CPU	Central Processing Unit
DMZ	Demilitarized Zone
DoS	Denial of Service
PAM	Privilege Access Management
ITCSA	IT Compliance and Security Architecture
ITD	Information Technology Department
TCP/IP	Transmission Control Protocol / Internet Protocol
USB	Universal Serial Bus
VM	Virtual Machine