ADIB – Standard

Client Security Standard

STD-ITD-510

Date: 30th July 2023

Version: 7.1

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
7.1	30th July, 2023	Annual Review No Change	Annual Review
7.0	30th July, 2022	Updated control: IT SecOps shall ensure approved DLP agent is deployed, and ADIB Periodic reports shall be shared with IT GRC team	Process enhancement and ensure alignment with best practices
6.0	30th July, 2021	-Added additional client security agents' solutions -Added control: Client Master Images should have minimum set of security solutions along with Latest Operating System Updates. -Modified review cycle from Biannual to annual: ITCSA will perform annual review of installed software to ensure compliance	Process enhancement and ensure alignment with best practices
5.0	Publishing Date	Added control for: - Software that are not in the whitelist will be treated as blacklist - ITCSA will perform biannual review of installed software	To ensure compliance
4.1	Publishing Date	No change. Document is up t66o date	Process annual cycle review
4.0	Publishing date	Updated Standard statement section	To be in line with the current practice
3.2	Publishing date	NESA Security Control update	NESA Compliance
3.1	Publishing date	Conversion of the document to new approved STD template	New approved STD template being practiced

Prepared by	Approved by	Reviewed by
Governance Team	Head of IT Compliance and Security Architecture Head of Technology GRC	IT Governance Manager IT Security Compliance Engineer

Document Contents

1 Overview

The objective of this document is to define specification for information security controls of a client (desktop/ laptop) installed in ADIB network.

2 Applicability

This standard is applicable to UAE, Qatar, Iraq, UK & Sudan ITD environment

3 Standard Owner

Head of Technology GRC

4 Standard Statements

1. All ADIB machines shall be prepared with only ADIB master image approved by ITGRC

2. The Latest, updated Master Image shall contain necessary client security agents (i.e.; Microsoft Defender, Forcepoint DLP, Zscaler Proxy Agent, Imprivata, MacAfee Suite, Cisco NAC, Avecto, Blue Coat proxy agent; Based on applicability)

3. Client Master Images should have minimum set of security solutions i.e.; Antivirus, Data loss prevention, Proxy Agent along with Latest Operating System Updates.

4. All Software installed in ADIB / Subsidiary environment shall be from the list given in Appendix-A-SW White-listed Software. A copy of the original software along-with its previous versions would be maintained by authorized administrators, along-with required information and parameters, procedures, configuration details, and supporting software.

5. Audit trail shall be maintained for any software installation, deployment of service / security patches etc.

6. Any exceptions or divergence from this list shall be approved explicitly by the IT-GRC team / representative, by following the Standard Service Catalogue Request procedure, and would be installed by authorized administrators only.

7. Deployment & Rollback of any software, firmware, security / service pack updates on the clients shall be maintained, as per the change management process.

8. Users shall have only one client machine either desktop or Laptop, unless authorized otherwise.

9. Client shall run only ADIB licensed software.

10. Non-business-related software such as Games, chat -software, etc. shall not be allowed.

11. All external storage devices (such as CD/DVD, floppy, USB) shall be disabled, unless authorized otherwise. For the authorized ones, ITD shall ensure scanning of the removable media for malware every time it is connected to ADIB's IT environment as per ADIB defined policies

12. Authorized security agents (such as Network Admission control, Single sign On, Device Control, Antivirus, DLPetc.) shall be deployed on all clients, while windows firewall shall be disabled.

13. System lock-out after ADIB defined idle time period shall be configured.

14. It’s the user’s responsibility to regularly connect their laptop to Authorized network to update their antivirus software signatures and Operating System.

15. Client shall not have any local accounts other than built-in accounts, unless otherwise authorized.
16. Default IDs such as administrator, guest etc. shall be renamed and their passwords shall be changed.
17. Unnecessary default IDs, services, shares shall be disabled.
18. Client name shall not include function /IP address / Staff Name.
19. Clients shall be added to appropriate Organization unit as per job role and administrative hierarchy.
20. Client shall not be connected to any unsecured public networks.
21. Client hard drive shall have only single partition as per Windows 10 AIDB standards, unless authorized otherwise. The partitions shall be in NTFS format.
22. Hard drives of client systems shall be encrypted
23. Desktops Hard drives which are considered as critical by GISD and ITCSA should be encrypted such as Card Centre
24. Client shall boot only from Hard Disk unless otherwise authorized.
25. BIOS parameters shall be secured
26. Remote connectivity shall be disabled when the user is connected to ADIB network and vice versa
27. Remote desktop sharing shall be enabled only for client administrators and authorized users as per the business requirements.
28. Remote access to clients shall be via secure protocols.
29. Screen saver locking shall get activated as per ADIB defined idle time.
30. Users shall be given normal user privileges.
31. Administrator privilege user activity shall be logged.
32. The setting for Interactive logon “Does not require CTRL+ ALT+DEL” shall be disabled.
33. The client shall be updated with the latest service pack and patches as required by the Patch Management Standard (refer STD-ITD-507).
34. The Master Image (for laptops and / 5or desktops) should be reviewed & updated on a semi-annual basis. The image should be updated with:
    a. latest versions of all security agents
    b. all security and operating system patches
    c. updates for 3rd party applications and ADIB’s Business Applications
35. Identify and Disable system utilities for normal users.
36. Access to system utilities should be provided as per business need and subjected to standard service request process. It shall also be monitored for its usage.

37. Any software not in the whitelist will be treated as blacklist unless and until it is assessed & approved by ITCSA.

38. IT SecOps shall ensure that approved DLP agent is deployed, and same version and engine is maintained across. ADIB. Periodic reports shall be shared with IT GRC team. Quarterly review shall be performed by IT GRC.

39. ITCSA will perform annual review for all installed software to ensure compliance

5 Exceptions

Any deviation to the standard shall be documented along-with associated risks and shall be approved

6 Appendixes

Annex I: Acronyms

Abbreviation	Acronym
ITD	Information Technology department
CSA	Compliance & Security architecture