




Application Whitelisting Policy

Doc. Control Number	Version
SNL-19	0.3



Document Reference

Item	Description
Title	SNLC Application Whitelisting
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	25 March 2024
Revision-Date	25 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	25/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	27/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	27/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	13 July 2022	Muhaned Ali	First Release
0.2	28 May 2023	Muhaned Ali	The policy has been updated
0.3	25 March 2024	Muhaned Ali	The policy has been reviewed and updated



Contents

1. Overview	4
2. Scope	4
3. Policy	4
4. Compliance and Enforcement	4
5. Policy Review	5
6. Appendix A - Index of Authorized Software	5
7. Approval	6

1. Overview

This policy outlines the principles and guidelines for implementing Application Whitelisting within SNLC. Application Whitelisting is a security control measure that restricts the execution of software applications to only approved and authorized ones. The purpose of this policy is to enhance the SNLC's cybersecurity posture by preventing the execution of unauthorized or potentially malicious applications, thereby reducing the risk of security breaches and data compromise.

2. Scope

This policy applies to all SNLC assets and all SNLC employees. Application Whitelisting shall be applied to all information assets, including servers, workstations, laptops, and any other endpoints within SNLC's IT infrastructure. All software applications, libraries, and scripts running on information assets shall be subject to the application whitelisting control.

3. Policy

3.1 List of Authorized Software

- a) Maintain and regularly update an Index of Authorized Software containing a comprehensive list of approved software applications, libraries, and scripts authorized to run on the SNLC's information assets.
- b) The Index of Authorized Software shall include details such as software name, vendor, version, type, and signature status (e.g., digitally signed).

3.2 Approved Application Whitelisting Tools

- a) Utilize approved and effective application whitelisting tools capable of enforcing the application whitelisting policy across all endpoints.
- b) As an application Whitelisting control mechanism, SNL utilizes ManageEngine Desktop Central.
- c) Regularly review and update the application whitelisting tools to ensure compatibility with the latest operating systems and software updates.

3.3 Establishment and Dissemination of the Index of Authorized Software

- a) The IT security Team shall be responsible for creating and maintaining the Index of Authorized Software.
- b) Disseminate the Index of Authorized Software to all relevant personnel, including system administrators, IT support staff, and end-users.

3.4 Regular Review and Update of the Index of Authorized Software

- a) GRC Team shall conduct periodic reviews of the Index of Authorized Software quarterly to ensure its accuracy and relevance.
- b) Update the Index of Authorized Software promptly whenever new software is approved, or existing software is deprecated.

3.5 Enforcing Application Whitelisting

- a) The IT team shall configure application whitelisting tools to strictly enforce the execution of only approved software.
- b) Prevent users from disabling or bypassing the application whitelisting controls through appropriate technical measures.

3.6 Exceptions and Approvals

- a) All requests for adding new software to the Index of Authorized Software or exceptions to the application whitelisting policy must be submitted through the IT team.
- b) Requests for exceptions shall be reviewed and approved by the INFOSEC Team or a designated authority.

4. Compliance and Enforcement

4.1 Compliance with this policy is mandatory for all employees, contractors, and individuals with access to SNLC's systems and data.

4.2 Non-compliance with this policy may result in disciplinary action, including but not limited to retraining, suspension, termination, and legal consequences, as appropriate.

5. Policy Review

5.1 This policy will be reviewed on a periodic basis to ensure its continued relevance and effectiveness. Any updates or modifications to this policy shall be communicated to all relevant employees and stakeholders.

6. Appendix A - Index of Authorized Software

Software Name	Vendor	Version	Type	Signature Status
Microsoft Office	Microsoft	365		
Microsoft Visio	Microsoft	2019		
Microsoft Project	Microsoft	2019		
Norton Security	NortonLifeLock	22.24.2.6		
ManageEngine UEMS-Agent	ManageEngine	11.2.2328.1W		
Wazuh Agent	Wazuh	4.3.11		
Cisco Webex Meeting	Cisco	43.9.0.27194		
Zoom	Zoom	5.17.33775		
FortiClient VPN	Fortinet	7.0.7.0345		
Active@ KillDisk 23	LSoft	23		
Adobe Acrobat 64	Adobe	24.001.20615		
Bitvise SSH Client	Bitvise Limited	9.33		
Cisco Packet Tracer	Cisco	8.2.1.118		
Google Chrome	Google LLC	123.0.6312.59		
MobaXterm	Mobatek	23.6.0.5186		
Notepad++	Notepad++	8.6.4		
Oracle VM VirtualBox	Oracle	7.0.14		
PowerISO	Power Software Ltd	8.5		
Wireshark	The wireshark developer	4.2.3		
Wondershare EdrawMax	EdrawSoft	13.0.3.1081		
WinSCP	Martin Prikry	6.3.1		
iMonitor	iDirect			
iBuilder	iDirect			
iPerf				
PDFelement	Adobe			
Mlink Planner2				
Visual Studio Code				
AutoCAD				
PuTTY	By Simon Tatham.	0.80		
ZKTeco Biotime 8.5	ZKTeco	8.5		



7. Approval

Entity	Name	Signature	Date
V.P	Abdullah Al Shuhail		27/3/2024