



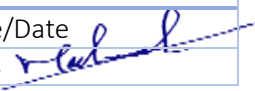
Acceptable Use Policy

Doc. Control Number	Version
SNL-11	1.2




Document Reference

Item	Description
Title	Acceptable Use Policy
Department	Cybersecurity Department
Version No	1.2
Status	Draft
Type	DOCX
Publish-Date	5 March 2024
Revision-Date	5 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	June 2020	Muhaned Ali	First Release
0.2	July 2021	Muhaned Ali	Updated and converted to a new format
0.3	18 May 2022	Muhaned Ali	A new control has been added
1.0	1 May 2023	Muhaned Ali	A new control has been added
1.1	6 November 2023	Muhaned Ali	Remote Users' Access has been added
1.2	5 March 2024	Muhaned Ali	Policy has been reviewed



Contents

1. Overview	4
2. Scope.....	4
3. Policy.....	4
4. Declaration.....	7

1. Overview

SNLC takes the subject of information security very seriously. We have a duty to protect the information that we collect and use for the benefit of the company and its customers. As an employee, you will be expected to comply fully with all the information security policies that are in place and to report any breaches of these policies of which you may become aware.

This policy gives a summary of the main points of the relevant policies and asks you to sign to say that you have read it and understand its provisions.

Anyone breaching information security policy may be subject to disciplinary action. If a criminal offence has been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, please seek advice from your immediate manager in the first instance.

2. Scope

This policy applies to all systems, people and processes that constitute the company's information systems, including board members, directors, employees, suppliers and other third parties who have access to SNLC systems.

3. Policy

4.1 General Clauses

- a) Information must be dealt with according to the specified classification and in accordance with the data classification policy and the data and information protection policy for SNLC in a manner that ensures the protection of information confidentiality, integrity, and availability.
- b) It is prohibited to infringe the rights of any person or company that is protected by copyright, patent, or other intellectual property, or similar laws or regulations; Including, but not limited to, installing unauthorized or illegal software.
- c) Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process, or access assets.
- d) Printouts on the Shared Printer must not be left unattended.
- e) External storage media must be kept securely and appropriately, such as making sure that the temperature is set at a certain degree and keeping it in a safe and isolated place.
- f) It is prohibited to use the password of other users, including the password of the user's manager or his subordinates.
- g) The safe and clean office policy must be adhered to, and the desktop, as well as the display screen, must be free of classified information.
- h) It is prohibited to disclose any information related to SNLC, including information related to systems and networks, to any unauthorized party, whether internally or externally.
- i) It is prohibited to disclose any policies, procedures, standards, or any kind of data related to Aramco with unauthorized entities or on the Internet.
- j) It is prohibited to publish information about SNL through the media and social networks without prior permission.
- k) It is prohibited to use the systems and assets of SNL for the purpose of achieving personal benefit and business, or to achieve any purpose not related to the activity and business of SNLC.
- l) Connecting personal devices to SNLC's networks and systems is strictly prohibited.
- m) It is prohibited to carry out any activities aimed at bypassing the protection systems of SNL, including anti-virus software, firewall, and malware without prior authorization, and in accordance with the procedures approved by SNLC.

- n) Users are personally responsible for protecting the data and information on the IT Resources being used by them. Users should not switch off any tools / services from the IT Resources set up by the IT Department like antivirus, firewalls etc.
- o) The Department Concerned with Cyber Security reserves the right to monitor systems, networks, and personal accounts related to work, and to review them periodically to monitor compliance with cyber security policies and standards.
- p) It is forbidden to host unauthorized persons to enter sensitive places without obtaining prior permission.
- q) At the time of resignation, Users should not send parting e-mail to all Users of SNL company this is strictly prohibited.
- r) Use of the e-mail service is monitored by the IT department to ensure that no illegal / offensive / criminal activities are being discussed over the corporate mail system. In the light of this monitoring ensure that all communication is restricted to business use.
- s) Using personal email to share and transmit Saudi Aramco is strictly prohibited.
- t) In the event of loss, theft, or leakage of information, the Cyber Security Department must be reported.
- u) The AUP shall be reviewed, measured, and optimized annually, and changes documented and approved.

4.2 Protecting Computers

- a) It is prohibited to use external storage media without prior permission from the Department concerned with cybersecurity.
- b) SNLC must implement a device control mechanism on Assets that are used to receive, store, process or transmit Saudi Aramco data, such as disabling the use of external storage media.
- c) User access to the operating system, applications and database must be reviewed on a semiannual basis to determine if accessing personnel still require such access.
- d) It is prohibited to carry out any activity that would affect the efficiency and safety of systems and assets without prior permission from the Department Concerned with Cyber Security, including activities that enable the user to obtain higher powers and privileges.
- e) The device must be secured before leaving the office by locking the screen, or signing out (Sign out or Lock), whether leaving for a short period or at the end of working hours.
- f) It is prohibited to leave any classified information inaccessible places, or to view it by unauthorized people.
- g) The IT Department will create two accounts for all PCs, one for administrators and one for standard users.
- h) All employees must have standard user access.
- i) For business reasons, all the technical team must have access to an admin.
- j) Allow the use of removable media based on business needs only.
- k) It is prohibited to install external tools on the computer without prior permission from the Department of Information Technology.
- l) The Department Concerned with Cyber Security shall be notified upon suspicion of any activity that may cause damage to the computers or assets of SNLC.

4.3 Acceptable Use of the Internet and Software

- a) In the event of suspicious websites that should be blocked, the Department of Cyber Security should be informed; Or vice versa.
- b) Remote administrative access from the Internet must not be allowed, unless explicitly approved, restricted, and controlled.
- c) You must ensure that intellectual property rights are not infringed while downloading information or documents for business purposes.
- d) Use of unlicensed software or other intellectual property is prohibited.

- e) Technology assets and systems connected to the Internet must be licensed and supported by the provider.
- f) A secure and authorized browser must be used to access the intranet or the Internet.
- g) Prohibit the use of technologies that allow bypassing a proxy or firewall to gain access to the Internet.
- h) It is prohibited to download or install software and tools on the assets of SNL without prior permission from the information technology department.
- i) It is prohibited to use the Internet for non-business purposes, including downloading media and files, and using file-sharing software.
- j) The Cyber Security Department should be reported when cyber risks are suspected, and security messages that may appear while browsing the Internet or internal networks should be treated with caution.
- k) It is prohibited to conduct a security scan for the purpose of discovering security vulnerabilities, including penetration testing, or monitoring of SNLC networks and systems, or those of third parties without prior authorization from the Department of Cyber Security.
- l) It is prohibited to use file-sharing sites without prior permission from the Department of Cyber Security.
- m) It is prohibited to visit suspicious sites, including hacking education sites.
- n) Unwanted software installation is not permitted.

4.4 Acceptable Use of e-mail and Communication System

- a) The use of e-mail, telephone, fax, or e-fax is prohibited for non-business purposes and in accordance with our Cyber Security Policies and Standards.
- b) Accessing the Email system from personal devices is not permitted.
- c) All personal emails whether received / sent / stored should be deleted immediately, in any case, before the end of every calendar month.
- d) Users should not send greetings / greeting cards via emails to other users within SNLC company.
- e) Using personal email to share and transmit Saudi Aramco data is strictly prohibited.
- f) Encryption techniques must be used when sending sensitive information via e-mail or communications systems.
- g) The email address of SNL must not be registered on any website that is not related to the business.
- h) The Cyber Security Department should be informed when there are suspicions of emails containing content that may cause damage to the systems or assets of SNLC.
- i) SNLC reserves the right to disclose the contents of e-mail messages after obtaining the necessary permits from the authorized person and the Department concerned with cybersecurity in accordance with the relevant procedures and regulations.
- j) Do not open suspicious or unexpected emails and attachments, even if they appear to be from trusted sources.

4.5 Video Meetings and Web-based Communications

- a) It is prohibited to use unauthorized tools or software to conduct video calls or meetings.
- b) It is forbidden to make calls or hold video meetings that are not related to work without obtaining prior permission.

4.6 Using Passwords

- a) All SNL Technology Assets and Systems must be password protected.
- b) Secure passwords must be chosen, and passwords for SNLC's systems and assets must be preserved. You should also choose passwords different from those of personal accounts, such as personal mail accounts and social networking sites.



- c) Sharing the password through any means, including electronic correspondence, voice communications, and paper writing is prohibited. Also, all users must not disclose the password to any third-party including co-workers and employees of the IT Department.
- d) You must change the password when a new password is provided to you by the system administrator.

4.7 Remote Users' Access

- a) The direct manager must approve remote access.
- b) All remote access should be documented, with the duration specified.

4. Declaration

I have read the information security policy summary above and agree to comply with its contents and those of any other relevant policies of which the company may make me aware.

Name of User: _____

Signature of User: _____ Date: _____