Reviewed On: 6/24/2022

Access Control Policy

Version 3.3

SILARIS INFORMATIONS PVT. LTD

ACCESS CONTROL POLICY

Version: 3.3

TITLE	ACCESS CONTROL POLICY	APPROVER (Signature)
Classification	Internal Use Only	
Document Number	ISMS_POL_30	
Author	Er. Tanay Dobhal	
Reviewer	Samarth Jain	
Approver	CEO- Ruumila Sadhu	
Document Owner	CISO / ISMS Manager	
Release Date	1st April 2013	
Reviewed date	24th June 2022	

ALTERATION HISTORY				
SR.NO	DESCRIPTION OF CHANGES	AUTHOR	ALTERATION DATE	VERSION
1	Initial Draft	Gursagar Preet	01-04-2013	V1.0
2	Review as per ISO 27001:2013	Gursagar Preet	01-04-2015	V1.1
3	Change the company Name	Gursagar Preet	01-04-2016	V1.2
4	Annual Document Review /ISO Audit Review	Gursagar Preet	01-04-2017	V1.3
5	ISO Audit Review	Rajesh Bisht	01-04-2018	V1.4
6	Document Review and Update	Rakesh Dhyani	14-03-2019	V2.0
7	Any third party external web URL links /applications must be	Er. Tanay Dobhal	13-03-2020	V2.1

	approved by ISMS team before sent for CEO approval.			
8	Hardware configuration management.	Er. Tanay Dobhal	16-03-2020	V2.2
9	Review as per ISO 27001:2013	Er. Tanay Dobhal	11-06-2020	V2.2
10	Operation access's review implemented (as per client requirement)	Er. Tanay Dobhal	22-08-2020	V2.3
11	DLP implementation on servers as per contractual requirements)	Er. Tanay Dobhal	15-10-2020	V2.4
12	Generic Login ID's provisioning for business/ Support requirements	Er. Tanay Dobhal	22-12-2020	V3.0
13	Generic Email ID's provisioning for business/Operation requirements	Er. Tanay Dobhal	05-03-2021	V3.1
14	Review as per ISO 27001:2013	Er. Tanay Dobhal	16-06-2021	V3.1
15	Review Of Email Approval Authority	Er. Tanay Dobhal	20-12-2021	V3.2
16	SME / ATL Designation Added	Er. Tanay Dobhal	13-04-2022	V3.3
17	Review as per ISO 27001:2013 (No Changes Required)	Er. Tanay Dobhal	24-06-2022	V3.3

1 Objective:

The following subsections outline the Access Control standards that constitute the access control policy. Each Silaris Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

2 Network Access Policy

This policy describes the security requirements for connections to Silaris internal systems and networks equipment's. It covers a wide variety of technologies including wire and wireless connections, dial-up modem links, Internet encrypted tunnels (also known as virtual private networks or VPNs), segmentation of network using VLANs, restricted access to network services, restricted physical access to network devices etc. All users, employees,

contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3

AC-1 Account Management:
All Business Systems must:

- Identify account types (i.e., individual, group, system, application, guest/anonymous, and temporary).
- Unique ID's for all employees shall be created for accesses (including but not limited to Windows/CRM/ Network ID/ETC.)
- In case generic Login ID's are required for any business/support requirements, in such case generic ID's shall be created against exception management policy.
- In case generic email ID's are required for any business/support requirement, in such case generic email ID's shall be created against exception management policy.
- Establish conditions for group membership.
- Identify authorized users of the information asset and specifying access privileges.
- Require appropriate approvals for requests to establish accounts.
  Establish, activate, modify, disable, and remove accounts.
- Specifically authorize and monitor the use of guest/anonymous and temporary accounts.
- WFH facility in which employees will be issued Silaris provided hardened laptop & desktops with internet dongles and secured AES-256-bit encryption VPN with 2FA & MAC binding protocol for connectivity to Silaris datacenter to maintain business continuity.
- Notify account managers when temporary accounts are no longer required and when information asset users are terminated, transferred, or information assets usage or need-to-know/need-to-share changes.
- Deactivate temporary accounts that are no longer required and accounts of terminated or transferred users.
- In case of any ITF / IJP (internal transfer formalities / Internal Job Posting), HR will share the information with IT team to revoke the employee all previous access.
- If all ID's created are not logged in within 24 hrs of creations shall get auto disabled & can only be unlocked against a ticket.
- If any ID's not in used for more than 90 days, then it will be automatically suspended and auto deleted after 180 days.

- Grant access to the system based on (1) valid access authorization, (2) Intended system usage, and (3) other attributes as required by the organization or associated mission/business functions.
- Operation's accesses shall be reviewed on quarterly basis as per client requirement.

AC-2 Information Flow Enforcement:

- All Business Systems must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with this policy.

AC-3 Separation of Duties:

All Business Systems must:

- Separates duties of individuals as necessary, to prevent malevolent activity without collusion.
- Document separation of duties.
- Implements separation of duties through assigned information asset access authorizations.

AC-4 Least Privilege:

- All Business Systems must employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

AC-5 System Use Notification:
All Business Systems must:

- Display an approved system use notification message or banner before, granting access to the system that provides privacy and security notices consistent with regulations, standards, and policies.
- Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information asset.

AC-6 Concurrent Session Control:

- All Business Systems must limit the number of concurrent sessions for each system account to **one** for information assets.

AC-7 Session Lock:

- All Business Systems must prevent further access to the information asset by initiating a session lock after 1**5 minutes** of inactivity or upon receiving a request from a user. In addition, Business Systems must retain the session lock until the user reestablishes access using established identification and authentication procedures.

AC-8 Permitted Actions without Identification or Authentication:

- All Business Systems must identify specific user actions that can be performed on the information asset without identification or authentication. In addition, Business Systems must document and provide supporting rationale in the security plan for the information asset, user actions not requiring identification and authentication.

AC-9 Wireless Access:

All Business Systems must:

- Establish usage restrictions and implementation guidance wireless access.
- Monitor for unauthorized wireless access to the information asset.
- Authorize wireless access to the information asset prior to connection.
- Enforce requirements for wireless connections for the information asset.

AC-10 Access Control for Mobile Devices: All Business Systems must:

- Establish usage restrictions and implementation guidance for Organization-controlled mobile devices.

- Authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information assets.

- Monitor for unauthorized connections of mobile devices to organizational formation assets.

- Enforce requirements for the connection of mobile devices to organizational information assets.

- Disable information asset functionality that provides the capability for automatic execution of code on mobile devices without user direction.

- Issue specially configured mobile devices to individuals traveling to locations (international locations which are considered sensitive by the Department of State) that the organization deems to be of significant risk in accordance with organizational policies and procedures.

AC-11 Remote Access:

- Remote access policy applies to network/system administrator to manage network remotely and vendors etc. accessing Silaris internal systems. For connectivity of any external network to connect to Silaris network, due approval is required from the CEO. Once Remote access requirement is approved by the CEO, end user has to raise a ticket with helpdesk or required configuration on his / her laptop/desktop.
- The connectivity has to follow secure and encrypted data transfer between Silaris and external network. To comply with this policy, we have following arrangements:

    - Remote access to internal network is provided by secure VPN tunnel established between two entities. Communication through VPN should be encrypted with at least 256 -bit encryption.
    - RDP Access: - RDP is being used to provide support in emergency. Access to server via RDP is restricted to specified user account.
    - Remote user is assigned a password that meets complexity standards.
    - Remote user is restricted to access only authorized applications and network resources in company's internal network by the means of VPN policy.
    - Remote user's system must have antivirus, anti-spyware and malware protected software installed and updated with latest security patches.

AC-12 Publicly Accessible Content: All Business Systems must:

- Designate individuals authorized to post information onto an organizational information system that is publicly accessible.

- Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
- Review the proposed content of publicly accessible information for Nonpublic information prior to posting onto the organizational information system.
- Review the content on the publicly accessible organizational information System for nonpublic information.
- Removes nonpublic information from the publicly accessible organizational information system, if discovered.

AC-13 - Physical Access:

- All network devices should be accessible by only authorized persons who are responsible for managing such devices and should be kept under secured place.
- All Network devices are secured in Datacenters.
- Only authorized users can access these devices by passing Bio-metric authentication used to secure the Datacenter, all access rights are reviewed on quarterly basis.
- CCTV cameras are being used in some of the datacenters to keep watch on physical access of network devices

AC-14 Logical Network Segmentation:

- Network Segmentation is required to maintain security and performance of the entire network.
- Network segmentation can prevent eavesdropping between segmented networks.
- To segment the Physical network, we have segmented our network with VLANs or logical separate networks as feasible.

AC-15 DLP:

1. Data loss prevention shall be installed on all MIS systems who receives & process the data.
2. DLP installation on production servers shall done as per contractual /clients requirements.
3. DLP shall be configured to block following critical accesses:-
   - Internet Access
   - Storage removal Devices
   - Cloud Storage
   - Customer PII information
   - Website Accesses (basis Access Control Policy approval process)
   - Print Screen Capture
   - Clip Board
   - Approved Email Access list
   - ETC.

4 Management VLAN is different from the Process VLAN.

- Servers and Network Devices are kept under Management VLAN or segregated domain wise.
- There are different VLANs or logical separate networks for each process to maintain efficient security and control over network resourced used by each process.
- Process users are restricted to specified applications and network resources by the means of VLAN assigned or separate logical network to them.
- MAC addresses binding enabled on all switches on the production floor.

5 Network Devices Management:

Special care must be taken while considering security of Network Devices Management via locally or remotely. All network devices must be physically secured in order to prevent unauthorized access to configuration or diagnostics ports. Remote access to configuration ports must be restricted by the means of strong passwords and via policy.

Console ports of Cisco and other network devices always configured with strong password.

No network device has default password set on its console or administrative port. Password of configuration ports changed on periodically basis.

6 CCTV Access Control:

The entire IP based CCTV surveillance system is design to control and monitor the entrance, server room, all processes etc. video management software shall offer both video stream management and video stream storage management.

- Only authorized surveillance team can enter inside the CCTV access zone after biometric clearance.
- Request for CCTV footage will only entertained by the surveillance team after the clearance (of CCTV access form) via admin team and verified by ISMS team. (form define in Silaris physical security policy).

Routing Policy:

Routing policy specifies the routing policy and routing protocols being used to maintain the smooth function of network. Routing policy & protocol defines the network stability and security of company's inter-network.

Static routes are being used to communicate within internal network and to connect to our remote sites. Static routes are considered most reliable and secure.

7 Information Access Policy:

Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

To comply with this policy, we have following arrangements:

- Access to critical network devices is only allowed to persons authorized by Manager – Networks.
- Access to critical devices is restricted by Biometric authentication or lock-in key and only authorized persons have access to these devices.
- Access to network devices is restricted via passwords and only authorized persons have credential information.

Email Id Creation Procedure:

- Once employee join the organization then their process / Dept. manager shall send mail for approval of creation of email id to HR- Backend / Process AVP or VP or HOD and at last IT – Head.
- After getting approval by respective authority then process manager need to create the ticket for creation of email id.
- Once ticket assigned and approval mail received by email support team then email support team will create email id.

Email Id Send / Receive Access Procedure:

- By default, the created email id shall without any send / receive accesses.
- Process Manager or Dept. head need to fill the official access approval form (ISMS_Doc_081).
- Once they filled then they need to send this form to email support team (Reason : There is the column number 9 which need to be filled by IT Dept. only, where they will mention that what send / receive accesses were given (if any) to him / her earlier.
- After filled the details, IT team will send back that form to process manager or Dept. head and then process manager or Dept. head will send that form to ISMS for security clearance.
- After ISMS clearance, process manager or Dept. head can proceed for CEO approval (with attachment of form).
- If CEO approve the access, then only IT team will provide him / her to demanded accesses.

8 Hardware Configuration Management:

All devices including Desktops and laptops are configured under AD environment (in addition to laptop policy).

Following policies are implemented:

- USB blocked
- Control Panel blocked
- Games Blocked
- Printer - Disabled
- Network disabled
- Command Prompt disabled
- Short cut keys disabled
- Restricted user login
- No access to install any software
- Anti-Virus Installed
- DLP on MIS system
- No access to share folders
- Concurrent Session
- Concurrent Session disabled
- No access to local HDD on agent's systems
- No C drive access to QA/TL/MIS/Managers

9 Access rights removable process:

The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, move from one department to another, contract or agreement, or adjusted upon change.

To comply with this policy, we have following arrangements:

- For laptop users, we remove MAC address of his/her laptop from all Wireless Access points.
- Data port used by employee is disabled.
- Change the password of the equipment's when any of the team members left the organization or any change in role & responsibilities of employment.

Physical access

- Disables the access on access control devices installed to restrict entry to critical areas like Datacenters etc.
- Disable or removes the telecom equipment provided
- Disable network port

Access through Network

- Disables or removes the domain / individual server logins provided to access ftp, home folders, shared folders, internet, VPN, printers or manage the network equipment and servers.
- FTP/SFTP shall not be used for any data transfers any exceptions shall be covered under Silaris Exception Management Policy.

Application access

- Disable removes or change the credentials or encryption key / certificate for access to emails, websites, databases, dialers, telecom equipment or manage the application servers.

Access through Internet

- Disable removes or change the credentials or encryption key / certificate for access to VPN connection, emails, websites, databases, dialers and network & telecom equipment.

Telephony access

- Disable removes or change the credentials for access to inbound numbers, Conference Bridge, remote barge-in facility and voice mail systems.

10 Clock synchronization Policy

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source. All systems has been synchronized with global standard clock.

11 Session-timeout Policy

Session-timeout policy specifies the inactive sessions shell be disconnected after an idle period of time to prevent any mishap while working on a remote management shell to save bandwidth in case not being used:

To comply with this policy, we have following arrangements:

Web server and any other application time out shall be between 20-25 minutes

We have default timeout setting for telnet/ftp and other network protocols in all Switches and Router.

Network Monitoring

All network devices, data center systems connected to network are being monitored for their availability, security and performance. Periodic review of Network logs is also carried out to detect any vulnerability or threat to Silaris network and systems.

User Access Rights and control procedure

This section describes the processes followed for granting, reviewing and removal of access rights of individual / group / organization starting, termination or change in employment or contract or agreement with Silaris. From the resources (internal and external) provided to individual / group / organization earlier during the course of their regular employment or contract or agreement with Silaris.

12 Information Resources

- Data Centers
- Applications, hosted within the premises or at third party premises like FTP, Websites, Databases, Emails etc.
- Network resources like shared folders
- Telephony resources, hosted within the premises or at third party premises like Bridge Conferencing, Remote barge-in etc.
- Network and Telecom equipment's & Network ports

13 Granting Access Rights:

New Employee

- All critical access like email / MS-Office/internet accesses is approved by the Business Head of Silaris. (CEO)
- Any third party external web URL links /applications must be approved by ISMS team before sent for CEO approval.

Standard Hardware Configuration Approved:

- Agent /SME / ATL/ TL/QC/ Asst. Manager and Above – Core 2 Duo (2-4 GB RAM,160-320 GB HDD)
- MIS – I3 and above
- Laptops – As per approval from CEO and IT Head

The employee's reporting manager or supervisor / business coordinator needs to send the request to IT through email or log the request in IT Helpdesk tool for providing the access to above mentioned resources. Depending on the department / process requirement, the access will be provided.

SME / ATL : SME / ATL designation shall be given on need basis career progression. The employee who are managing 15 and above TME shall get this designation after approved by CEO.

14 Access Matrix: -

Access Rights - Silaris Operations/Business Development Users											
User	**USB**	**Internet**	**Mails**	**QC Module**	**Dialer**	**DLP**	**CRM**	**FTP**	**Print**	**OS**	**Hardware**
Agent	NO	Client Approved Website	No	No	Yes	NO	Basic	No	NO	Win_10_Pro	Core 2 Duo
SME	NO	Client Approved Website	Restricted	No	Yes	NO	Basic	No	NO	Win_10_Pro	Core 2 Duo
ATL	NO	Client Approved Website	Restricted	No	Yes	NO	Basic	No	NO	Win_10_Pro	Core 2 Duo
TL	NO	Client Approved Website	Restricted	No	Yes	NO	Basic	No	NO	Win_10_Pro	Core 2 Duo
QC	NO	Client Approved Website	Restricted	Yes	No	NO	Basic	No	NO	Win_10_Pro	Core 2 Duo
MIS	NO	Client Approved Website	Restricted	No	No	Yes	Restricted Admin	Client Approv e	NO	Win_10_Pro	I-3 and Above
Asst.Mgr/ Managers	NO	Client Approved Website	Restricted	Yes	No	NO	Admin	NO	NO	Win_10_Pro	Core 2 Duo / Laptop
AVP & Above	NO	Restricted	Restricted	Restricted	NO	NO	NO	NO	NO	Win_10_Pro	Laptop
IT User Access List											

User	USB	Device/Server /Monitoring Tool	Internet	Mails	FTP	DLP	RDP		Print	OS	Hardware
IT Executives	NO	Restricted Servers Access	No	Restricted	NO	NO	NO		NO	Win_10_Pro	Core 2 Duo
Network Admin	NO	Router/Firewall / Switches/ Monitoring Tool	Restricted	Restricted	NO	NO	NO		NO	Win_10_Pro	I-3 and Above
System Admin	NO	Servers / Monitoring Tool	Restricted	Restricted	NO	NO	NO		NO	Win_10_Pro	I-3 and Above
Mgr. & Sr.Mgr	NO	Admin Privileges	Restricted	Restricted	NO	NO	NO		NO	Win_10_Pro	I-3 and Above
AVP & Above	NO	Admin Privileges	Restricted	Restricted	NO	NO	NO		NO	Win_10_Pro	Laptop
HR Function Users Access List											
User	**USB**		**Internet**	**Mails**	**FTP**	**DLP**			**Print**	**OS**	**Hardware**
Executives & Above	NO		Job Portals	Restricted	NO	NO			NO	Win_10_Pro	Core 2 Duo
Asst.Mgr & Manager	NO		Job Portals	Restricted	NO	NO			NO	Win_10_Pro	Core 2 Duo
Sr.Mgr & GM	NO		Job Portals	Restricted	NO	NO			NO	Win_10_Pro	Core 2 Duo
AVP & Above	NO		Job Portals	Restricted	NO	NO			NO	Win_10_Pro	I-3 and Above /Laptop
Admin Function User Access List											
User	**USB**		**Internet**	**Mails**	**FTP**	**DLP**			**Print**	**OS**	**Hardware**
Executives & Above	NO		Advertisement /Electronics/Gov	Restricted	NO	NO			NO	Win_10_Pro	Core 2 Duo
Asst.Mgr & Manager	NO		Advertisement /Electronics/Gov	Restricted	NO	NO			NO	Win_10_Pro	Core 2 Duo

Sr.Mgr & GM	NO		Advertisement /Electronics/Gov	Restricted	NO	NO			NO	Win_10_Pro	Core 2 Duo
AVP & Above	NO		Advertisement /Electronics/Gov	Restricted	NO	NO			NO	Win_10_Pro	I-3 and Above /Laptop

15 Share Drives and Folders

Share drives and Folders are not permitted until its business critical requirement, access to any share drive / folder must be approved by the CEO and VP-IT with Silaris exception management policy

16 Change in Access Rights:

Change in employment such as inter-department movement / promotion/ demotion resignation / termination or Absconding, trigger revision of access rights. The employee / employee's reporting manager or supervisor / business coordinator / vendor needs to send the request to IT through email or log the request in IT Helpdesk tool for any change in current access rights, which needs to be approved by department / process manager or supervisor / IT head, whichever is applicable.

Removal of access rights

- As soon as an employee is leaving the organization he/she brings the F&F form for getting the clearance from IT, all the access rights for (CRM/ Dialer and e mail etc.) will be revoked before the form is signed by the designated authority.
- HR will also share the list of all absconding and terminated employees to IT and Admin on regular basis and IT team will ensure to log a ticket and review all access list, in case any id is still active then rights are revoked and ticket is closed

Review of user access rights

- All access rights will be reviewed on quarterly basis, which is designed to positively confirm all users including vendors and clients. Any lapsed or unwanted access rights, which are identified, will be disabled immediately and will be removed unless positively reconfirmed.

The review will be conducted as follows.

- List of users will be generated on the basis of access rights to the resources.
- Any user not confirmed will have his/her access to the resources removed.
- Any change found in access rights to the user should be rectified.

17 Exception Handling

Requests for exceptions to this policy shall be addressed to and approved by CISO/ Equivalent. Exceptions granted shall be issued a policy waiver for exceptional cases and defined period. At the completion of the case / time period, the need for the waiver shall be reassessed and re-approved, if necessary.

Access Granted to CEO/CFO/CIO are exception to this policy.

_____*_____*_____

Document Review:

This policy document will be reviewed whenever there are significant changes or at least once in a year.