Reviewed On: 6/24/2022

Acceptable Usage Policy

Version 2.2

SILARIS INFORMATIONS PVT. LTD

ACCEPTABLE USAGE POLICY

Version: 2.2

TITLE	ACCEPTABLE USAGE POLICY	APPROVER (Signature)
Classification	Internal Use Only	
Document Number	ISMS_POL_02	
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	Social Media Usage	Er. Tanay Dobhal	02-07-2019	V2.1
8	Review as per ISO 27001:2013	Er. Tanay Dobhal	11-06-2020	V2.1
9	Review as per ISO 27001:2013	Er. Tanay Dobhal	01-06-2021	V2.1
10	Review Of Email Id creation, Approval Authority	Er. Tanay Dobhal	20-12-2021	V2.2

11	Review as per ISO 27001:2013 (No Changes Required)	Er. Tanay Dobhal	24-06-2022	V2.2

1 Objective:

The purpose of this document is to raise user awareness and make personnel accountable for information they access, use, store, process, and/or transmit. The document is a guideline that every member of Silaris should follow both insider and outside their work environment.

2 Policy Statement:

All the employees, contractors, consultants, temporaries, and other workers should adhere to the acceptable usage of facilities that are owned or leased by the company such as work stations, Email and Internet provided to them, that in-turn facilitate for a secure and productive working environment"

3 ISO 27001:2013 reference:

- A.6.2.1 - Mobile device policy
- A.6.2.2 - Teleworking
- A.8.1.2 - Ownership of Assets
- A.8.1.3 - Acceptable use of assets
- A.8.2.3 - Handling of assets
- A.9.3.1 - Use of secret authentication information
- A.16.1.2 - Reporting information security events
- A.16.1.3- Reporting information security weaknesses
- A.11.2.6 - Security of equipment and assets off-premises
- A.11.2.9 - Clear desk and clear screen policy

4 Legal Requirement:

- Indian Act – Information Technology Act (2000)

5 Definition of Information Assets

Information is defined as anything having business value. Examples of information are personally identifiable information (PII), customer, Silaris pricing, employee, financial, operational, communication, intellectual property and security information or any other information that can harm Silaris image, reputation or risk to revenue.

6 Responsibility

It is the responsibility of all users within and outside the organization to ensure protection of all kind of information and related infrastructure assets. This includes protection of confidentiality, integrity, and availability, as it relates to their areas of work.

7 General Security Practices

- Under no circumstances is an employee of SILARIS authorized to engage in any activity that is illegal under local, state, country or international law while utilizing SILARIS -owned resources.
- Employees are forbidden to talk about SILARIS business sensitive issues with anyone outside of SILARIS without due authorization.
- In certain business context, where authorization may not be feasible, employees are required to exercise caution and judgment before disclosing any information.

7 Physical Security

Mobile computing devices of any kind including but not limited following to are not allowed inside the restricted area unless approved by management due to business requirements.

- Smartphones
- Other mobile/cellular phones
- Tablet computers
- Portable media devices
- PDAs
- Ultra-mobile PCs (UMPCs)
- Laptop/notebook computers, including home desktops
- Any personally-owned device capable of storing organizational data and connecting to a network
- Camera's
- Data Cable /USB drive/flash media/Bluetooth device are strictly not allowed to be connected with any laptop / Desktop.
- Silaris facilities are strictly NO SMOKING/Drinking Zone.
- Smoking is only permitted at designated zones
- Eatables are only allowed within the canteen area / outside the premises.
- Mobile devices are strictly not allowed on production floors.
- All Tele callers must submit their mobile devices to their respective TL/Managers.
- All TL/Managers must ensure that all mobile devices collected should be locked in secured lockers provided by the admin team.
- Pen & paper are not allowed on production floor; under no circumstances teams on production floor should carry pen & paper on the floor.
- Printer & Scanners are not authorized on production floors and can only be installed against business requirements with due approvals with Silaris Exception management policy.

8 User ID & Password Protection:

User Identification (user ID) and Passwords are the keys to access your information. The following guidelines are recommended to protect you and the organization against any breach related to identity disclosure.

Passwords naming and storage:

- Passwords shall be minimum 8 characters long and shall contain alphanumeric characters with special characters. Avoid using known names such as spouse name, date of birth, kids name and pets name as others easily guess them for unauthorized access.
- Password good example: Sam@1295
- Password bad example: sam1295
- By making passwords complex you are making it difficult to be compromised.

Password Responsibility:

- Users are responsible for the security of their passwords and accounts. Passwords should be changed every 30 days for Domain Users. Password should not be written down on media (such as paper), except for lodging with departmental security staff or secure safekeeping, where appropriate. Password should be changed as per the Silaris policy and whenever there is any indication of possible system or password compromise.

9 Usage of Electronic Mail (email)

- Email communication is a business necessity for all kind of communications whether internal or external. The usage of emails also brings several risks, as it is one of the most vulnerable mediums for several recognized and often unknown threats. SILARIS expects that the following security controls are exercised by individuals in order to prevent any security incident arising from usage of email.

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.

Disclaimer:

- All Emails sent by employees should have a disclaimer stating that "the opinions expressed are strictly their own and not necessarily those of SILARIS, unless posting is in the course of business duties. The disclaimer should also state that
- Internet communication is unsafe and that the individual and the organization hold no liability in case the mail is being modified during the transmission".

- **Email from Unknown Sources:** Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, Malware, spy ware, or Trojan horse code. These threats have a potential to compromise systems and network and therefore user caution is an extremely important.

- **Emails containing SPAM:** When employees receive unwanted and unsolicited email (also known as SPAM), they must refrain from responding directly to the sender. Instead, they should forward the message to the system administrator who will take steps to prevent further transmissions.

- Employees must treat electronic mail messages and files as "Confidential" information. Electronic mail must be handled as a "Confidential" and direct communication between a sender and a recipient.

- SILARIS electronic mail system is to be used only for business purposes. All messages sent by electronic mail are SILARIS records. SILARIS reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose.

10 **Prohibited Actions Using Email**

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

- Any form of harassment via email, telephone or sms, whether through language, frequency, or size of messages.

- Unauthorized use, or forging, of email header information.

- Use of unsolicited email originating from within SILARIS networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by SILARIS or connected via SILARIS network.

- While sending classified information as attachments, you are requiring to zip the file and send the password through 'out of band' methods. Out of band refers to any medium than user for sending the primary medium. An example is mobile text, or a voice call.

- Mail size is restricted to 5 MB only. Exceptions will be for Silaris Senior management only. Any other exception will need approval from CEO of the organization.

Sensitive File

- Any file which have confidential information should be password protected.

Sensitive File sharing over email

- It is always a good idea to send a password protected zip file with password sent over other mediums, such as sms or spoken over voice.

Email Signature

An email signature is a small block of text appended to the end of an email in order to identify the sender. All employee of Silaris shall create an email signature.

Internal Standard:

The email signature will consist of the employee's name, employee's designation, official title: department / Process / office name, employee's office phone number (optional).

Example:

Name:

Designation:

Process/ Dept. / Office Name:

Phone Number: (Optional)

External Standard:

The email signature will consist of the employee's name, employee's designation, official title: department / Process / office name, employee's office phone number (optional), Silaris Address, Silaris Logo.

Example:

Name:

Designation:

Process/ Dept. / Office Name:

Phone Number: (Optional)

Address:

Logo:

Employees may not create their own variations or interpretations of the official email signature style for outgoing email. Employees may not add information, including links to other websites or social media accounts, to their official email signature.

11 Usage of Office Network & Communication Infrastructure

Office Network & Communication Infrastructure has been provided in order to ensure optimum communication between employees and business partners. The systems include business applications, operating systems, Databases, and host of internal and external network related services. SILARIS expects that the following security controls are exercised by individuals in order to prevent security incidents arising from the usage and administration of Network & Communication Infrastructure

- Anti-Virus Protection: All hosts used by the employee that are connected to the SILARIS Internet/Intranet whether owned by the employee or SILARIS, shall be continually executing approved virus-scanning software with a current virus database, unless overridden by departmental or group policy. If users have administrative rights on their workstations ensure that passwords are never disabled. Users shall be held responsible in case a system is found without anti-virus

protection disabled especially in those machines where the user has administrator access.

- Violations of the rights of any person or Silaris protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SILARIS .

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SILARIS or the end user does not have an active license is strictly prohibited. Employees should not save games, jokes, mp3s or any such information for entertainment purposes.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. Do not share your access credential at work with any other employees.

- Using SILARIS computing asset to actively engage in procuring or transmitting material that is in violation of business code of conduct sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Making fraudulent offers of products, items, or services originating from any SILARIS account.

- Scanning the network with the purpose of exploiting the weakness is strictly prohibited.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet.

- Circumventing user authentication or security of any host, network or account.

- Employees are forbidden from using SILARIS electronic communication system for charitable endeavors, private business activities or amusement/entertainment purposes.

12 Usage of Desktop:

Desktops are the primary medium of system interaction for most users. Users are responsible for the security of their allocated desktops. SILARIS expects that the following security controls are exercised by individuals in order to prevent security incident from the usage of desktops.

- Screensavers: All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at <10> minutes or less, or by logging-off (Windows + L) when the host will be unattended.

- Employees are forbidden to use any messenger/chat applications such as (but not limited to) like MSN Messenger, Yahoo messenger, ICQ etc. unless explicitly permitted.

13 Usage of Notebook/Laptop:

Note book/Laptop Computer is the primary medium of system interaction for almost all users outside the office locations. Users are responsible for the security of their allocated Notebooks. SILARIS expects that the following security controls are exercised by individuals in order to prevent security incident from the usage of Notebook Computers:

- Because information contained on portable computers is especially vulnerable, special care should be exercised to protect information from being gleaned by others in a public place. Using Notebook PCs in public places (conferences, training rooms etc.) calls for additional physical security, usage of Laptop Locks is advised.

- Employees should not connect directly to the Internet via modem, GPRS or any other mean's except by Silaris issued devices such as laptops while on SILARIS premises.

- Laptop/note book have a continuous threat of theft as they are easily visible. Avoid using laptop bags that suggest the laptop inside. If not keep in close custody. There have been incidents related to laptop thefts inside the car. Avoid getting tricked by incidents that drive your attention around the car when someone can open your door and pick up your laptop in a fraction of seconds.

14 Connecting to Internet from Public places

Users are required to take special caution while outside the office network. While connecting to any public hotspot/wireless connection, ensure that the connection is secure. This can be visible by simple clicking on the properties link of any available link. Avoid insecure links as they are potential for man in the middle attack and an attacked can sniff all your communication.

In case you need to access to access and the only option is an insecure network (such as an airport) do not perform any task that require submitting your credentials on a plan http:// website? A secure website https:// would be safer.

15 Secure usage of mobile devices

- Mobile device contain Silaris information in the form of emails and documents, therefore they should always be protected physically as well as logically.
- Physical protection involves keeping the device in proximity to the individual.
- Logical protection involves keeping the devices protected by a password and session time out after 5 minutes.
- In case the mobile device is lost report immediately to the issuing department or the security manager in order to stop further relay of messages.
- Also read vendor (Apple, Android) driven guideline for secure remote destruction of content if the control is applicable.

16 Secure usage of physical access cards

- Physical access cards are issued to individuals to access sensitive locations.
- The access control policy defines access based on 'need to know' and in this case 'need to enter'.
- It is mandatory to carry and display the physical access cards at all times.
- In case the access card is lost report immediately to the issuing department or the security manager.

17 Secure usage of cryptographic keys

- Cryptographic keys (such RSA token) are used as an additional layer of authentication to access sensitive applications.
- It is mandatory to possess the issued cryptographic key at all times.

18 Internet usage policy

- Internet access is made available based on business requirement.
- For those roles/personnel that have been given access, users are required to exercise restraint.
- Visiting websites that are not official are strictly prohibited.
- If you need additional access to websites other than those presently provided, seek approval from your reporting manager/business head.
- SILARIS has monitoring controls in place to track internet usage.

19 Clear Desk and Clear Screen Policy

- All personnel are required to ensure that paper documents/files, other assets are kept in lock and key, when no longer in use;
- All personnel are required to lock their screen (Pressing Windows + L or Control-ALT-DEL) when no longer working in their PC/notebook;
- Group policy enforces screen lock every 15 minutes. If you are moving away from your screen press Windows + L to lock your screen on windows machines and **Control + Shift + Eject** on Mac machines with an optical drive. (**Control + Shift + Power on a mac machine with no optical drive)**

20 Teleworking Policy

- Teleworking is only applicable In case of an EPIDEMIC/ PANDEMIC/ENDEMIC situation Silaris shall invoke WFH facility in which employees will be issued Silaris provided

hardened laptop & desktops with internet dongles and secured AES-256-bit encryption VPN connectivity to data center for BCP.

- Mobile Applications may also be provisioned for business continuity.

21 Social Media/Social networking Policy

While using social media such as (but not limited) twitter/Facebook/linked-In avoid disclosing information that reflects organization performance in anyway. Avoid using any language comment that can damage the image and reputation of the organization.

Every Employee of Silaris, regardless of his/her organizational unit or form of employment, Will comply with all of the following:

- To realize that what is said as a private person may be understood as spoken on behalf of Silaris.
- To remember that he/she is an Employee of Silaris and take care not to mislead his/her readers into thinking that he/she is speaking on behalf of, whether or not he/she mentions to SILARIS in the post.
- To avoid stating his/her personal opinions or views in a way that may be interpreted as a public statement made on behalf of SILARIS.

22 Compliance with applicable laws and regulations and SILARIS

- To comply with laws and regulations, and SILARIS regulations, and not to infringe any Intellectual property right or other right of others.
- To be honest and responsible
- To be responsible for what he/she has posted.
- To realize that his/her post may be seen by an unspecified large number of people and respect that reader may make their own individual interpretations on his/her post.
- To be aware that highly emotional communication is very likely to prolong useless argument increase misunderstanding and make the situation worse.
- To respect the rights of the person he/she is posting about and the opinions of his/her readers.
- Not to post anything that offends accepted social standards of decency.
- To respect the confidentiality of certain information
- Not to post any personal or confidential business information about SILARIS or SILARIS stakeholders.
- Not to post any information that is not publicly available and is learned in the course of his/her jobs.
- To realize that information once posted online cannot be deleted

- To realize how fast information spreads online
- A public blog is not the place to communicate Silaris policies to Silaris employees
- Respect copyright laws. Always protect sensitive information, such as protected acquisition and personally identifiable information.
- Do not publish or report on conversations that are meant to be pre--decisional or internal to Silaris unless given permission by management.
- Remain focused on existing commitments, and achieving Silaris's mission. Your use of social media tools should never interfere with your primary duties, with the exception of where it is a primary duty to use these tools to do your job.

23 Log Review and Analysis

SILARIS has a policy on conducting user log reviews on systems and infrastructure. These logs review reveal user behavior on systems and infrastructure.

24 Usage of Flash Media (USB drive)

Usage of USB/flash memory is strictly prohibited in the organization. In case of data file transfer, which cannot be made through other mediums, ensure formal approval is in place before such media can be used.

25 Usage of classified documents

Any document identified as confidential or internal use only should be strictly handled based on the documented procedure. In case sensitive documents needs to be transferred or destroyed, this should be done under the formal approval of the document owner or the head of department – to which this document belongs.

26 Weakness & Incident Reporting

A security weakness /incident may be a result of compromise to Confidentiality, Integrity, and availability, Non-repudiation and/or Legal or Contractual Non-conformity. The impact of any security incident may result in serious consequences to the business and therefore an adherence to this policy is to avoid any such serious incident.

- Employees should be well aware of Incident reporting procedures and understand areas, which may or may not be reported.

- Employees must promptly report all information security alerts, warnings, suspected vulnerabilities, weaknesses, and the like to the Information Security Manger using the incident reporting Form/Procedure.
- Users are prohibited from utilizing SILARIS systems to forward such information to other users, whether the other users are internal or external to SILARIS .

27 Areas that can be reported are as follows (not exhaustive):

Any event or weakness that can jeopardize the confidentiality, integrity and/ availability' of information assets is worthy of reporting. This can include physical controls, technology controls, personnel behaviors related to information assets, and procedural controls.

An example of each of these is give below:

Physical controls

Can cover all aspects of physical security such as weak doors, access control systems, entry and exit areas, and associated processes.

Technical controls

Can cover strengths and weakness such as password complexity (less than 6), lack of antivirus, email attachments, accidental or deliberate mass mails etc.

Personnel controls

Such as unauthorized access attempts, violation of Silaris policy, violation of internet usage policy etc.

Administrative controls

Such as asset not identified, document classification, no documentation, no change and access definition etc.

Note that an employee can report his/her head of department/reporting manager. Alternatively one can also approach the Information Security officer by phone, or email at isms@silaris.in

28 Consequence Management/Disciplinary action Procedure (DAP)

The policies are designed to protect organizational and employee interest. However if an employee violates the policy terms, he/she is subject to disciplinary action.

29 Intellectual Property/ownership

SILARIS owns all hosted infrastructure including information stored, processed, and transmitted in the Silaris offices. No employee can claim the content or intellectual property of the assets/hosted infrastructure as his or her own.

30 Right to audit

All Silaris owned infrastructure is owned by SILARIS, and SILARIS has the right to audit any part of the infrastructure at any point of time, without employee notice. This is to ensure that in case of a security event, the organization would need evidence to demonstrate compliance, and if necessary bring the guilty to the court of law, the guilty can be insider or outsider to the organization.

31 Question/clarifications/improvements

If you have any questions, clarifications or improvements please do not hesitate to call IT Helpdesk or write an email to: isms@silaris.in

Document Review:

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