

Internet & Email Policy

**Version History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. No.** | **Release Date** | **Description of Change** | **Authored / Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 30th May 2020 | Initial draft | Rahul Raj |  |  |
| 1.0 | 22nd July 20 | Baseline and published | Rahul Raj | Tim | Shankar/Joe |
| 2.0 | 11th Match 21 | Restructured the document. Rename section 5, 5.1 and 5.2. Add section 5.3, 5.4, 5.5, 5.6 and 5.7 | Rahul Raj | Tim/Tanuj |  |

**Table of Contents**

[1. Objectives 4](#_Toc70357281)

[2. Scope 4](#_Toc70357282)

[3. Internet and E-mail Policy 4](#_Toc70357283)

[3.1 Internet Access/Usage Policy 4](#_Toc70357284)

[3.2 E-mail Usage Policy 4](#_Toc70357285)

[4. Computer, Email, Internet Usage &Information Security Guidelines 5](#_Toc70357286)

[5. Policy Elements 7](#_Toc70357287)

[5.1 Inappropriate use of Internet and company E-mail 7](#_Toc70357293)

[5.2 Appropriate use of Corporate Email 8](#_Toc70357294)

[5.3 Personal Use of Official Email Account 8](#_Toc70357295)

[5.4 Use of Non-SVAM domain email and Messaging Apps 8](#_Toc70357296)

[5.5 Email Security 9](#_Toc70357297)

[5.6 Email Signature 9](#_Toc70357298)

[5.7 Disciplinary Action 10](#_Toc70357299)

[5.8 Email Ethics 10](#_Toc70357300)

# Objectives

Internet access and usage policy has been devised keeping in mind the vulnerabilities that an Internet connection exposes the corporate networked environment. It aims at educating users about ‘what to’ and ‘what not to’ be done while accessing the Internet. Our goal is to protect our confidential data from breaches and safeguard our reputation and technological property.

# Scope

Internet access and usage policy applies to all the Employees, Vendor / Third Parties, and Business Partners who are assigned (or given access to) a corporate Internet or email.

# Internet and E-mail Policy

## 3.1 Internet Access/Usage Policy

* Internet access to the employees is provided for business requirement of SVAM
* Approval from the functional/departmental head will be obtained for extra access privileges for any employee.
* Employees of SVAM with Internet access will not participate in Internet discussion groups, chat rooms, or other public social sites.
* Any information or software downloaded from the Internet will be screened through virus detection software before being used and prior approval from IT Team.
* Employees will deter from transmitting ‘Confidential’ or ‘Restricted’ information over the Internet without prior management approval and reasonable security measures (such as encryption or other appropriate method) in place.
* IT department will be responsible for installing appropriate software to restrict websites sites that can be visited. The audit log contains information about sites that are accessed and reviewed by IT department.
* IT department will be responsible for managing the service provider for any outsource services including but not limited to ISP, VPN, Antivirus, AMC Vendors etc.

## 3.2 E-mail Usage Policy

* Employees located at customer sites should adhere to the e-mail usage policies of the client.
* Email protection will be protected from unauthorized access by using Spam filter (barracuda) and Sonicwall Firewall (cloud physical)
* Communication through e-mail medium should not be unethical and improper.
* Confidentiality will be maintained for the official/business data/information that needs to be transmitted via e-mail communication.
* Employees and other users of e-mail and communication systems of SVAM will use them for official and business purpose only.
* Internal mails as well as mails to business partners and third-party vendors will be sent using official e-mail accounts only.
* Employees will include a standard disclaimer in the ‘signature’ to be appended to each email.
* Users will not create or forward chain letters, or mails that can be deemed to be spam/junk, using their official e-mail account.
* Employees will not use official e-mail accounts for sending and receiving personal e-mail messages.
* All messages distributed via the company’s Email system are Company’s property. Anyone using the email service consents to this monitoring.
* Network Administrator will block Email addresses, which are causing unnecessary computing burden on Mail Server like Spam mails, mailing lists, and newsletters.
* Network Administrator will put limit on size of incoming and outgoing mail messages for employees is (which is 10 MB), for functional head is (which is 20 MB) and for IT admin is (which is 50 MB). Exceptions for management.
* No mail originating from SVAM domain will be unethical, abusive, use illicit language and/or infringe copyright or other legal regulation.
* No individual can send email to [allindia@svam.com](mailto:allindia@svam.com) to protect the unauthorized and unethical mass mailing service within the Organization. Only department head can send email to all India/US.

# Computer, Email, Internet Usage &Information Security Guidelines

All employees shall sign Internet and email usage policy and kept with HR file, respectively.

* Appendix A: For SVAM INDIA refer to Guideline “GD-26-ISMS-CEI-SVAM INDIA-Computer Email and Internet Usage Guidelines”
* Appendix B: For SVAM US refer to Guideline “GD-27-ISMS-CEI-SVAM-Computer Email and Internet Usage Guidelines”

# Policy Elements



## Inappropriate use of Internet and company E-mail

Using Internet inappropriately will be against the company’s policy and will be strictly avoided. Inappropriate use includes but not limited to:

* Sign up for illegal, unreliable, disreputable, or suspect websites and services.
* Send unauthorized marketing content or solicitation emails.
* Register for a competitor’s services unless authorized.
* Send insulting or discriminatory messages and content.
* Intentionally spam other people’s emails, including their coworkers.
* Accessing, downloading, or forwarding pornographic or illicit material.
* Solicitations for any purpose, which are not expressly approved by management.
* Revealing or publicizing proprietary or confidential information.
* Representing personal opinions as those of the company.
* Making or posting indecent remarks.
* "Flaming" (e.g., malicious written attacks) or similar written attacks.
* Uploading or downloading commercial software in violation of its copyright.
* Downloading any software or electronic files without reasonable virus protection measures in place.
* Intentionally interfering with the normal operation of SVAM Internet gateway/proxy machine.
* Enter into contractual agreements via the Internet on behalf of the company.
* Use or possess Internet scanning or security vulnerability assessment tools, such as SATAN or ISS, without the permission of the Manager IT.
* Use the company logos or the company materials in any web page or Internet posting unless the company management has approved it, in advance.
* Attempt to inappropriately telnet to or port scan remote systems on the Internet.

## Appropriate use of Corporate Email

Employees can use their corporate email for work-related purposes without limitations. For example, employees can use their email to:

* Communicate with current or prospective customers and partners.
* Log in to purchased software they have legitimate access to.
* Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
* Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

## Personal Use of Official Email Account

E-Mail accounts that are sponsored by SVAM or clients are not allowed to be used for personal purposes except for few exceptions like

* Register for classes or meetups.
* Send emails to friends and family if they do not spam or disclose confidential information.
* Download eBooks, guides, and other content for their personal use as long as it is safe and appropriate.

Employees must always adhere to this policy, in addition to our [Data Confidentiality and Protection Policy](https://svam.sharepoint.com/:w:/s/SVAM-SoftwareEngineeringProcessGroupSEPG/EYrok1d1MqZIv5RHercWhO4BIX7LsjB8HPpOUNCzOVsydQ?e=AqXgn6).

## Use of Non-SVAM domain email and Messaging Apps

The use of non SVAM email accounts or Applications (such as Gmail, Yahoo, Hotmail or similar) and messaging applications (such as Facebook Messenger, Snap Chat, Me, or WhatsApp similar), for official related business poses a security risk, prevents the proper management of records, and is prohibited.

Limited exception approved by line manager to allow an employee or a group of employees to use a non SVAM email account in certain situations (e.g., in emergency, disaster, IT systems limitations) provided adequate systems and processes are in place to ensure that resulting records are captured by IT manager for record keeping systems. Such emails shall be created & monitored by IT team.

When we are communicating through a non SVAM domain email account or any external email account that relates to official business it must be treated as a company record. Same email id with different client communication should be prohibited.

Rules for creation Non SVAM Email account: When considering how to compile your email address, you should use a format with the end goal in mind.

* Don’t be fancy, keep it standard.
* Leave Nicknames to personal communication.
* **DO NOT USE** Client Contact Person Name/Client Business Name for creating email account as well as display name.
* Combine your name. ex-

First name + last name = cliffordchi@domain.com

First name . last name = clifford.chi@domain.com

First name . middle name . last name = clifford.douglas.chi@domain.com

First initial + last name = cchi@domain.com

First initial + middle name + last name = cdouglaschi@domain.com

First initial + middle initial +last name = cdchi@domain.com

## Email Security

Email is often the medium of hacker attacks, confidentiality breaches, viruses, and other malware. These issues can compromise company reputation, legality, and security of equipment. Employees must:

* Adhere to [Password Policy](https://svam.sharepoint.com/:w:/s/SVAM-SoftwareEngineeringProcessGroupSEPG/Ebp7kqIUdSFFkS0TFm-QkGABcgwCa_S6KHq_s1N14jic3A?e=p2qpkh)
* Remember passwords instead of writing them down and keep them secret.
* Change their email password every 90 days.
* Also, employees should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:
* Avoid opening attachments and clicking on links when content is not adequately explained (e.g., “Watch this video, it’s amazing.”)
* Be suspicious of clickbait titles.
* Check email and names of unknown senders to ensure they are legitimate.
* Look for inconsistencies or style red flags (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)
* If an employee is not sure that an email, they received is safe, they can contact to IT Team.

## Email Signature

SVAM encourage employees to create an email signature that exudes professionalism and represents our company well. Salespeople and executives, who represent our company to customers and stakeholders, should pay special attention to how they close emails. Here is a template of an acceptable email signature:

*[Employee Name]*

*[Employee Title], [Company Name with link]*

*[Company Address]*

*[Phone number]*

Employees may also include professional images, company logos and work-related videos and links in email signatures.

## Disciplinary Action

Employees who don’t adhere to the present policy will face disciplinary action up to and including termination. Example reasons for termination are:

* Using a corporate email address to send confidential data without authorization.
* Sending offensive or inappropriate emails to our customers, colleagues, or partners.
* Using a corporate email for an illegal activity.

## Email Ethics

* E-mail should be checked at least once a day.
* Always have a subject heading which reflects the content. The following qualifications can be added:
  + URGENT: Addressee, please act within 48 hours.
  + VERY URGENT: Please take immediate action.
  + FYI: For your information only.
* Addressees and carbon copies (CCs) should be carefully selected.
* Readability should be ensured by:
* Not using capitals and unnecessary punctuation.
* Spell check of e-mails.
* Not using fancy fonts, graphics etc.
* Attachments should be avoided when the text can be put in the message itself. Using RTF or HTML format allows copying most office documents into the message itself.