**Communication Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

# 

# **Purpose**

The purpose of this policy is to detail the acceptable communication ways in *[Company]*.

# **Scope**

This policy applies to all *[Company]* employees, contractors, third parties who access internal information and business processes.

# **Policy**

## **Email Communication**

* Employees should use the company's email account only for business purposes.
* Employees should not use or access an email account assigned to another employee to send or receive messages.
* Employees should not download/forward attachments that are from an unknown or unreliable source.
* Employees should not create or send malicious attachments by email.
* Employees are encouraged to limit the use of the Reply-All function in any approved email client.
* The only approved email client is Google. Use of any other client is prohibited.
* Employees should not forge or try to forge email messages.
* Employees should not disguise or attempt to hide their identity while sending email messages.
* Employees should not use their personal email accounts for sending official mail. All official email communication should take place only via an official email account.
* Employees should not create their own or forward externally provided email messages which may be considered to be harassment or which may create a hostile work environment.
* Suppose a user faces profane, obscene, or derogatory remarks in an email. In that case, he/she should communicate with the sender, ask him/her to stop sending such messages, and report such offensive emails directly to the management.
* Employees should not automatically forward their emails to any address outside the company’s networks.
* Employees should write well-structured emails and use short, descriptive subjects. The use of Internet abbreviations and characters such as smileys is not encouraged.
* Employees should use the spell checker before sending out an email.
* Employees should not write emails in capitals.
* Employees should mark emails as significant only if they are important.

## **Messengers usage**

* Employees should use only approved messengers like Google Chat, Slack.
* Employees should not use the work profile for personal use.
* The same communication rules as for emails apply here as well.

## **Blogging and social media**

* Blogging and social networking by *[Company]* employees are subject to the terms of this policy, whether performed from the corporate network or personal systems. As a representative of *[Company]*, blogging and social networking must be formally approved by the CEO before use. In blog or website, including blogs or sites published from personal or public systems, should company business matters be discussed, or material detrimental to the company be published. The user assumes all risks associated with blogging and social networking.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. IT Manager shall exclusively perform changes to this policy.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. *[Company]’s* management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Data Classification Policy