Everest engineering

Electronic messaging policy

ISM.08

Version 0.2.3

July 1 2025

Contents

1 Introduction

This policy document outlines how Everest Engineering electronic messaging facilities may be used and behaviours that are not permitted. It applies to all use of these facilities whatever the means or location of access e.g. via mobile devices or outside the office.

Electronic messaging covers email and other forms of instant and store-and-forward messaging such as SMS, messaging apps, and messaging facilities within social media platforms.

1.1 Scope

This policy applies to all Everest Engineering permanent employees, contractors, advisors and contracted partners using, or granted access to, information assets and information processing facilities owned by Everest Engineering, our customers (whether contracted or not) and third party partners.

2 Electronic messaging policy

2.1 Sending and receiving messages

Only Everest Engineering provided electronic messaging facilities may be used when communicating with others electronically on official business. Personal accounts may not be used. Communication must adhere to the data security classification scheme.

Messages from an organisation address should be considered in the same way as other more formal methods of communication. Nothing must be sent externally which might affect Everest Engineering's reputation or affect its relationships with suppliers, customers or other stakeholders.

2.1.1 Retention

All messages sent from an organisation account remain the property of Everest Engineering and are considered to be part of the corporate record. All organisation messages should be considered as official communications from the organisation and treated accordingly.

We take our employees privacy seriously. However, the organisation maintains its legal right to monitor and audit the use of electronic messaging by authorised users in order to comply with local lws. This will be done in accordance with the provisions of relevant legislation.

Deletion of a message from an individual account does not necessarily mean that it has been permanently removed from the organisation's IT systems and such messages may still be subject to audit and review.

2.1.2 Cultural considerations

Be aware that it cannot be guaranteed that a message will be received or read by a recipient and that messages can be interpreted in different ways according to the culture, role and even prevailing mood of the individual reading it. You should therefore always consider whether the use of electronic messaging is an appropriate means of conveying the information involved and whether an alternative such as the telephone would be preferable, particularly if the message is urgent or complex.

You must avoid sending unnecessary messages to distribution lists, particularly those with a wide circulation such as a global list of all employees. Where required, such messages should be sent via Everest Engineering's communications department.

2.1.3 Prohibited use

Official organisation electronic messaging facilities must not be used:

- for the distribution of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations;
- to send material that infringes the copyright or intellectual property rights of another person or organisation;
- for activities that corrupt or destroy other users' data or otherwise disrupt the work of other users;
- to distribute any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material;
- to send anything which is designed or likely to cause annoyance, inconvenience or needless anxiety to others;
- to convey abusive, threatening or bullying messages to others;
- to transmit material that either discriminates or encourages discrimination on the grounds of race, gender, sexual orientation, marital status, disability, political or religious beliefs;
- for the transmission of defamatory material or false claims of a deceptive nature;
- for activities that violate the privacy of other users;
- to send anonymous messages; and
- for any other activities which bring, or may bring, the organisation into disrepute.

2.1.4 Junk messages

You should delete any unsolicited junk messages or spam you receive without clicking on links. Do not reply to the message as this can confirm the existence of a valid address to the sender, resulting in further unwanted communication.

2.2 Email

Auto-forwarding of emails should not be used if there is a possibility that this may result in sensitive information being forwarded to a recipient that does not have enough security clearance for the level of information involved.

Where possible, make use of links to files within email messages rather than attaching a copy of the file, particularly if the email message has a wide distribution. This will prevent other user's mailboxes from filling up and so avoid consequent disruption.

Computer viruses, adware and other malware may be inadvertently downloaded and installed via received emails. The organisation provides anti-malware software that runs on every computer that has access to the network in order to protect endpoints. If you believe you may have a virus, or you have been sent an email that may contain one, please report this to Everest Engineering's IT service desk immediately. Do not open any attachments you believe may contain a virus.

If a computer virus is deliberately or accidentally sent to another organisation, Everest Engineering could be held liable if the transmission could be considered negligent. Therefore, you must not:

- transmit by email any file attachments which you know to be infected with a virus;
- download data or programs of any nature from unknown sources;
- disable or reconfigure the installed anti-malware software operating on a computer used to access email facilities; and
- forward virus warnings other than to the Everest Engineering IT service desk.