IHS EMAIL POLICY – User Information

This document describes the Email policy at IHS. Please read it carefully. You will find rules as well as hints which settings could be adjusted for your personal account, too.

Definitions used in this document

- Local Email: Any email originated from a PC in the IHS LAN by means of a trusted client software (e.g. Outlook, Thunderbird) and sent to an IHS address as final recipient. Local mail is considered to be trusted mail.
- Other Email: Any email that is not considered to be trusted. This is email where at least one of the following applies:
    - Sent with webmail
    - Sent from a client connected to the DMZ (yellow cable)
    - Sent via "IHSVPN"
    - Sent from a WLAN client
    - Recipient is not an IHS email address

Local Email

This email is not subject to the restrictions of the Email Policy implemented on our mail gateway servers as it does not leave our LAN. However, there is a pitfall: If the recipient has configured his/her account to forward mail to an external address, the email does leave the LAN and therefore has to pass our mail gateway. This means one cannot be sure that an email is a local one until it has reached all final recipients. Therefore, you are encouraged not to attach banned files (see below). If you want to send files to other IHS members instead write them an email pointing them to the place from where they can copy it (e.g. U:\userid\public or U:\userid\group). If the contents of your file are confidential so that you cannot save it on a place where someone other may have access to it, then use WinZip to compress it and attach the zip - file.

Email Policy on Gateway Servers (Other Email):

Virus Detection

Each mail is scanned for viruses on our mail gateways. If a virus is detected, the email is blocked and a notification message is sent back to the sender if the virus is not in the list of "known viruses that fake sender address".

Banned Files

If an attachment is part of the Banned File Class the complete email is blocked and a notification is sent back to the sender. An attachment is part of the banned file class if either its name is in the banned file names or its type (data format) is found in the banned file type list.

Banned file names: (Name includes one of the following extensions, eg: filename.**exe**.)

- ade
- adp
- bas
- bat
- chm
- cmd
- com
- cpl
- crt
- exe
- hlp
- hta
- inf
- ins
- jar
- isp
- js
- jse
- lnk
- mdb
- mde
- msc
- msi
- msp

- mst
- pcd
- pif
- reg
- scr
- sct
- shs
- shb
- vb|
- vbe
- vbs
- wsc
- wsf
- wsh

Banned file types:

- application/x-msdownload
- application/x-msdos-program

Spam detection

Each email is scanned for patterns indicating that it might be Spam and its score ("hit value") is calculated. If the hit value is equal or greater than the "kill value" the email is discarded. If the hit value is equal or greater than the "spam value" but less than the kill value, the header is changed to "*****SPAM*****" followed by the original subject. The following table shows the overall picture with default values (spam value = 5.3, kill value = 100):

Hit value (x)	Action
x < 5.3	Mail is passed
5.3 <= x < 30	Mail Subject is modified and passed
30 <= x	Mail is blocked

If you want the default spam and hit value to be adjusted for your account please contact mailadm@ihs.ac.at.

False positives and negatives:

False negatives are Spam mails not classified as Spam (hit value is below spam value). A false positive is a legitimate mail classified as Spam (hit value is equal or greater than spam value).

To train the filtering software and improve the results, you are asked to copy false positives in a mailbox "_SpamError" and move false negatives into a mailbox "_SpamNotDetected".

Note: forwarding such emails to someone of the IT department is of no help, since the headers of the email (usually hidden by your email software) are lost and they are necessary for training.

In addition, please report false positives by sending an email to mailadm@ihs.ac.at.

If you expect to regularly receive emails from organizations where you already got a false positive or negative, consider having this address added to a allow- or blocklist (see below).

Block and Allowlists:

A blocklist contains sender addresses which should always be treated as spammers. In fact this adds 100 points to emails received from this address.

A allowlisted sender address is never tagged as Spam.

If you want to add an address to your allow- or blocklist please contact mailadm@ihs.ac.at.

Note: If you have an address listed in both, block and allow, emails received from this address will be delivered always, but tagged as Spam.