

## **Mail Transaction Policy of NICNET**

### **Purpose:**

The purpose of this policy is to establish the base of mail transaction within and outside NICNET.

### **Scope:**

This policy applies to all servers owned and/or operated by National Informatics Centre and to servers registered under any National Informatics Centre owned Network Domain

### **Policy:**

**IMPORTANT: No Mail server can be configured in NICNET, prior to approval from the Messaging Group and Security Group. Servers configured without approvals will be disconnected. This applies to NIC servers and mail servers under projects. Project coordinators need to take prior clearance, if a server is being configured.**

#### **LIMITS AT MAIL GATEWAYS**

- All outgoing and incoming mails from and to NICNET shall enter and leave the Network through the SMTP Gateway.
- All mails, incoming/outgoing will be checked for virus and possibility of Spam.
- Anti-relay options will be enabled on all mail servers. Servers configured as open-relay shall be disconnected from the Network, without any warning.
- All servers in NICNET are configured for a Maximum of **16 MB** message size (this includes message header, all attachments encoded into printable ASCII characters) only.
- Mails will stored at the SMTP gateways for a period of 5 days only. Mails not delivered within 5 days will be deleted from the gateway.

#### **LIMITS FOR MAIL CLIENTS**

- Max recipients allowed per mail is **50**.
- Max message size can be attached using Outlook Express/WEB browser to the mail is **8MB**.
- Maximum size of a decompressed file is **40MB**
- Max decompressed file count (maximum number of files in a zipped archive send along with the e-mail as attachment) is **100**
- Maximum no of attachments is **50**
- Mailboxes of users occupying more than **70 MB** in their INBOX will be deleted. Users are advised to move important mails to a folder. Restoration requests will NOT be entertained.

**NOTE: Recipient will NOT get any notification of a missed mail,**

- if the mail intended for him/her exceeds the above set of limits.
- if the mail intended for him/her has a virus.
- if the mail intended for him/her is a Spam.

**Spam Handling:** In order to fight against SPAM, we have installed spam filtering tool called Spam Prevention Solutions (SPS) from Trend micro. Whenever a mail is detected as spam by SPS, we add a prefix “**sopa9m:**” to subject so that mail delivery program down the line puts them into a separate folder called “**Probably Spam**”.

**Attention:** Hence users are requested to check their “**Probably Spam**” folder once a day, as mails with false Spam positives can be stored in this folder.

**Exception:** In case you do not accept our spam prevention policy, you may ask for an exception. On a written request from you, we will put in a white list of users. There by none of your mails will be scanned by the software.

**If a mail is missed, the possible reason can be one of the following:**

- (1) **Blocked by Trend Micro E-manager Content Filter Policies:** which are based on From(Sender:) & To(Recipient:), Subject:, Attachment:, some combinations of these in order to satisfy the guidelines issued by **Security Division NIC**.

***NOTE:** The mails that are dropped based on “**Subject: Rule**” need not have the exact subject line. A variation of the same can also cause a mail to be filtered out; hence users should avoid using similar subject lines.*

**Content Filter Policies**

```
DOM=IS"ms38.hinet.net"
FROM=IS"<>"
FROM=I"support@microsoft.com"
SUBJ=IS"Garden of eden"
SUBJ=IS"I want special deals"
SUBJ=IS"game"
SUBJ=IS"[CaCOaCa] Sheikh Abdulaziz Bin Baz"
SUBJ=IS"tool"
SUBJ=IS"NOSHADE"
SUBJ=IS"viagra"
SUBJ=IS"endspan"
SUBJ=IS"Bikini "
FROM=IS"jky@yahoo.com"
SUBJ=IS"$Home Loans!... Debt Consolidation... Refinance.."
SUBJ=IS"Weight Loss"
SUBJ=IS"no Boss "
DOM=IS"telek.ru"
FROM=IS"m_thompson_ci@telnor.net"
FROM=IS"jhne9k82l@yahoo.ca"
FROM=IS"ifs5z9sfy@aol.com"
```

FROM=IS"lpyzpe2oy0u7@hotmail.com"  
TO=IS"garlic@mgci.com",FROM=I"n@yahoo.com"  
SUBJ=IS"myro maintainablity "  
SUBJ=IS"Mortgage "  
SUBJ=IS"casino "  
SUBJ=IS"free movies"  
SUBJ=IS"increase big why"  
FROM=IS"management@solutions-intg.com"  
DOM=IS"gmx.at",FROM=IS"zewellfranz@gmx.at"  
SUBJ=IS"BANNED CD"  
SUBJ=IS"Re: Movie"  
SUBJ=IS"Re : Application"  
SUBJ=IS"Fw: INSHA ALLAH "  
FROM=IS"ashe@panamsolutions.com"  
FROM=IS"djpStockMarketAlert45654@yahoo.com"  
ATTACH=IS"sample.exe:all"  
ATTACH=IS"readme.exe:all"  
SUBJ=IS"Fwd: So cool a flash,enjoy it"  
SUBJ=IS"Fwd: Increase Your Length"  
FROM=IS"obihia\_nduka2003@indiatimes.com "  
FROM=IS"johnsimon@pkobp.pl "  
FROM=IS"cityshopping@rediffmail.com"  
SUBJ=IS"Re: Movies"  
FROM=IS"roncaj3502@eudoramail.com"  
FROM=IS"deglacier614421@dublin.com"  
FROM=IS"ost-123@onlinesuccesstoday.com"  
FROM=IS"bobby@abutus.com"  
FROM=IS"covered10945faces@yahoo.com"  
FROM=IS"playbunny13215girl@yahoo.com"  
FROM=IS"-@saturnnet.com"  
FROM=IS"xxx29806dating@yahoo.com"  
FROM=IS"johnwilson@yahoo.com "  
FROM=IS"nancy6209@desertedeals.com"  
FROM=IS"jayant\_patil@yahoo.com"  
FROM=IS"Zoe@FAR-AWAY-PLACES.COM"  
FROM=IS"Prizes@offers.traveljini.com "  
ATTACH=IS"update.exe:all"  
ATTACH=IS"toolbar.exe:all"  
ATTACH=IS"wizard.exe:all"  
ATTACH=IS"support.exe:all"  
ATTACH=IS"Shakira\_1997\_part\_1\_.Mpeg\_.scr:none"  
FROM=IS"janinagharris\_li@voila.fr"

FROM=IS"c02g7@pacbell.net"  
FROM=IS"cbrln261e@aol.com"  
FROM=IS"lucia@whiteoutmedia.com"  
FROM=IS"rzgvjgfani@bscinet.com"  
FROM=IS"bgiuvvy@lycos.com"  
FROM=IS"ida@infolandfill.com"  
FROM=IS"FierceDesignsn7w@provided2ubyu.com"  
FROM=IS"ipnofrqizbln@yahoo.com"  
FROM=IS"customersupport@mx17.hardlyaplace4u.com "  
FROM=IS"wbdjl@sancharnet.in"  
FROM=IS"41462681076@dumb-n-fun.com "  
FROM=IS"chrisjustice12@netscape.net"  
FROM=IS"big@boss.com.kar.nic.in"  
FROM=IS"dpnatusobi@masrawy.com"  
FROM=IS"wbdjl@sancharnet.in "  
FROM=IS"quotation@verba-volant.net"  
FROM=IS"EmanusShafto@in-box.net"  
FROM=IS"caldwell\_fb@azlyrics.com"  
FROM=IS"jobreplacement@mx17.grizzlydeers.com "  
FROM=IS"vmittal@pathinfotech.com"  
FROM=IS"oreos@42promotions.com "  
FROM=IS"ie-72640259-5468\_2109867501@b.mrhmail.com"  
ATTACH=IS" PROFORMA.doc.scr .scr:none"  
FROM=IS"proformacorp@proformacorp.com"  
SUBJ=IS"NEVER WORRY ABOUT SEPTIC TANK MAINTENANCE AGAIN! "  
ATTACH=IS"lovegirl.exe:all"  
FROM=IS"newsletter@shaadi.com"  
ATTACH=IS"coconut.exe:all"  
FROM=IS"bi01p1.co.us.ibm.com"  
ATTACH=IS".pif:all"  
ATTACH=IS".scr:all"  
ATTACH=IS"patch.exe:all"  
SUBJ=I"Re: Your application"  
SUBJ=I"Re: Approved"  
SUBJ=I"Re: Re: My details"  
SUBJ=I"Re: Details"  
SUBJ=I"Your details"  
SUBJ=IS"Re:wicked  
screensaver",ATTACH=IS"movie0045.pif,wicked\_scr.scr,application.pif,document\_944  
6.pif,details.pif,your\_details.pif,thank\_you.pif,document\_all.pif,your\_document.pif.:all"  
SUBJ=IS"Re: Your application",  
ATTACH=IS"movie0045.pif,wicked\_scr.scr,application.pif,document\_9446.pif,details.p  
if,your\_details.pif,thank\_you.pif,document\_all.pif,your\_document.pif.:all"

SUBJ=IS"Re:  
Approved",ATTACH=IS"movie0045.pif,wicked\_scr.scr,application.pif,document\_9446.  
pif,details.pif,your\_details.pif,thank\_you.pif,document\_all.pif,your\_document.pif.:all"  
SUBJ=IS"Re: Re: My  
details",ATTACH=IS"movie0045.pif,wicked\_scr.scr,application.pif,document\_9446.pif,  
details.pif,your\_details.pif,thank\_you.pif,document\_all.pif,your\_document.pif.:all"  
SUBJ=IS"Re: Details",  
ATTACH=IS"movie0045.pif,wicked\_scr.scr,application.pif,document\_9446.pif,details.p  
if,your\_details.pif,thank\_you.pif,document\_all.pif,your\_document.pif.:all"  
SUBJ=IS"Your details",  
ATTACH=IS"movie0045.pif,wicked\_scr.scr,application.pif,document\_9446.pif,details.p  
if,your\_details.pif,thank\_you.pif,document\_all.pif,your\_document.pif.:all"  
SUBJ=IS"Thank you123!",ATTACH=IS".:all"  
SUBJ=IS" Virus Warning Message"  
SUBJ=IS"nooutboundnotifications"  
SUBJ=IS"noinboundnotifications"  
ATTACH=I"Account Invoice.Doc.exe:all"  
ATTACH=I"Invoice.Doc.exe:all"  
ATTACH=I"Account Update.Doc.exe:all"  
SUBJ=IS"Fraudulent escrow service",ATTACH=IS"INFO.zip:all"  
SUBJ=IS"Mail delivery failed: returning message to sender."  
SUBJ=IS"hey..",ATTACH=IS"Popup.exe:none"  
SUBJ=IS"Speed up your connection!",ATTACH=IS"t\_dsl.exe:none"  
SUBJ=IS"Mail delivery failed: returning message to  
sender",ATTACH=IS"message.vbs:none"  
FROM=IS"mailerform@microsoft.net"  
FROM=IS"xjsfvtfzsgq-hipvv@bulletin.ms.com"  
FROM=IS"qtwgrxhkww@confidence\_msn.net"  
SUBJ=IS"Cracks!",ATTACH=IS"CrkList.exe:all"  
SUBJ=IS"The patch",ATTACH=IS"Patch.exe:all"  
SUBJ=IS"Last Update",ATTACH=IS"LUPdate.exe:none"  
SUBJ=IS"Do not release",ATTACH=IS"pack.exe:all"  
SUBJ=IS"Beta",ATTACH=IS"\_SetupB.exe:all"  
SUBJ=IS"Help",ATTACH=IS"Source.exe:all"  
SUBJ=IS"Evaluation copy",ATTACH=IS"Setup.exe:all"  
SUBJ=IS"Pr0n!",ATTACH=IS"Sex.exe:all"  
SUBJ=IS"Roms",ATTACH=IS"Roms.exe:all"  
SUBJ=IS"Documents",ATTACH=IS"Docs.exe:all"  
SUBJ=IS"Hacker Hunter",ATTACH=IS"Hacker\_Hunter.exe:all"  
ATTACH=IS"Q993934.exe:all"  
FROM=IS"support@microsoft.com",SUBJ=IS"Microsoft Windows  
Patch",ATTACH=IS"install.exe:all"

```
FROM=IS"msn@microsoft.com",SUBJ=IS"Support
Message",ATTACH=IS"MSNUPDATE.exe:all"
FROM=IS"woawenehsr-ohofw@bulletin.ms.net",SUBJ=IS"Newest Internet Security
Upgrade",ATTACH=IS"QONGR.exe:all"
SUBJ=IS"Current Net Security Pack"
SUBJ=IS"Current Net Security Pack"
SUBJ=IS"latest security upgrade"
SUBJ=IS"latest security upgrade",ATTACH=IS"upgrade.exe:all"
SUBJ=IS"New Internet Security Update"
SUBJ=IS"Critical Update"
SUBJ=IS"Newest Net Critical Patch"
SUBJ=IS"latest net patch"
SUBJ=IS"Latest Net Critical Update"
FROM=IS"admin@mp.nic.in"
FROM=IS"admin@ua.nic.in"
FROM=IS"admin@chdut.nic.in"
ATTACH=IS"readnow.zip:all"
TO=I"alluser@hub.nic.in"
```

## (2) **Heuristic Filtering: (part of Spam Prevention Solutions from Trendmicro)**

Spam Prevention Solution is a high-performance anti-Spam application designed to protect NICNET from Spam at the gateway.

Spam Prevention Solution is designed to defeat Spam using heuristics rules technology—a technology that offers more adaptable and “future-proof” protection against the ever-changing tactics of spammers.

Policy-based configuration options allow administrators to assign variable catch rate sensitivities based on Spam category and user groups, along with flexible Filter Actions for appropriate message disposition options. Spam Prevention Solution can delete, quarantine, tag based on Spam likelihood level.

Heuristics rules technology monitors, evaluates, and identifies suspicious email traffic to determine a Spam probability based upon collectively weighted and contextually evaluated characteristics.

As messages pass through the system, the SPS heuristic filter applies thousands of rules against the message envelope, the header, and the content. Each rule is assigned a numerical value, and an equation is formulated based on the weighted significance and the combination of rules that are triggered. The result of this equation is the Spam score.

SPS makes a decision on whether the message is Spam or valid by measuring the Spam score against the desired level of Spam sensitivity. Setting the sensitivity higher causes more messages to be considered Spam, since increased sensitivity means that a lower Spam score will result in a message being considered Spam. **Categories of Spam**

If the heuristic Spam filter categorizes a message as Spam, it will usually fall into one of four categories:

- **Sexual content: Adult or pornographic material**
- **Racist content: Racially insensitive material**
- **Make Money Fast: Get-rich-quick material**
- **Commercial offer: Sale notices, coupons, and special offers**

The Baseline Detection Rate and the category settings allow the system to derive a sensitivity level based on your company's tolerances.

The Baseline detection rate is used to determine the overall sensitivity to messages that are potentially Spam. Regardless of how individual category sensitivities are set, the Baseline detection rate provides a general level of protection against Spam. Increasing the setting of one or more of the categories increases the sensitivity to that type of content.

The Baseline detection Rate and category sensitivity levels are set independently, but parameters from both settings provide the final sensitivity level that determines whether the message is categorized as spam. Category sensitivity levels multiply the Baseline detection rate and increase the likelihood that a message that triggers a category setting will be considered Spam.

If the Spam score for a given message exceeds the sensitivity level of your policy, the message is considered Spam. There are three exceptions to this:

- **if the sender appears on the “Approved Senders list”, the message is never considered Spam.**
- **If the sender appears on the “Blocked Senders list”, the message is always considered spam.**
- **If text in the message triggers a “Text exemption filter”, the message is never considered to be Spam.**

The heuristic Spam filter determines whether a message should be evaluated for each of the four categories before performing the actual evaluation. Changing a category sensitivity level will not have any effect unless the message is evaluated in that category. Consider the following example of a partial message header from a message that was categorized as spam because it triggered the ‘ Commercial’ category:

```
X-imss-result: Commercial_LeastConfident
X-imss-scores: Clean:0.0003 C:42 M:2 S:5 R:5
X-imss-settings: Baseline:4 C:3 M:3 S:4 R:3 (0.1000 0.3000)
X-pstn-settings: 3 (1.0000:3.0000) smCr
```

#### **Understanding the imss-result line**

The first line in the above example show the heuristic Spam filter category that the message triggered. If a message does not trigger the heuristic Spam filter, this line will say ‘ passed ’. In the above example, the message triggered the ‘ Commercial’ category, and the level of confidence was ‘ Least confident’.

#### **Understanding the imss-scores line**

The second line above shows the spam scores assigned to this message. The first number is the Clean score, and the other four numbers represent the four categories. In the case of

the message represented above, the ' Commercial' category score was 42, the ' Make money fast' score was 2, and the ' Sexual content' and ' Racially insensitive' scores were both 5.

### **Understanding the imss-settings line**

The third line in the example represents the heuristic Spam filter settings at the time the message was processed. The Baseline number represents the setting for the Baseline detection rate and the other letters represent the sensitivity settings for the categories. The final two numbers are the baseline threshold and the triggered category threshold. When evaluating messages, the heuristic Spam filter first determines what category a message was most likely to fall into. In the case of this example, the category was ' Commercial' . You can verify which category SPS chose by checking the imss-scores line and seeing which category has the highest number.

Based on the above, users should avoid using subjects like:

Workshop, Meeting, Hello, test mail, mail check, lets meet, etc.

They should check their "Probably Spam" folder on a daily basis

### **(3) Signature Spam:**

Certified Spam and drooped as it is based on a predefined database inside SPS (Spam Protection Solutions from Trend Micro), and mails under this head are guaranteed Spam.

### **(4) Advanced content filter:**

Mails under this head will have the following in their content:

Profanity	Global Policy
1	Racial Discrimination
2	Sexual Discrimination
3	Hoaxes
4	Chainmail
5	Love Bug
6	Block HTML script messages