


INTER PLANT STANDARD – STEEL INDUSTRY		
 IPSS	GUIDELINES FOR ORGANISATIONAL EMAIL SETUP	IPSS:2-08-004-13

0.0 FOREWORD

- 0.1. This interplant standard has been prepared by the standards committee on Information & Communication Technology, IPSS 2:8, with the active participation of the representatives of the steel plants, major consulting organizations and established manufacturer and was adopted in June, 2013.
- 0.2. It is important requirement for Steel Industry like other Industries to prepare Guidelines for Organizational Email Setup.

1.0 SCOPE

- 1.1. This document is intended to assist in planning, configuring and maintaining mail servers and mail clients.
- 1.2. The document, while technical in nature, provides the background information to help readers understand the topics that are discussed. The intended audience for this document includes the following:
- 1) Users when setting up mail clients and accessing email
 - 2) System engineers and architects when designing and implementing mail systems
 - 3) System administrators when administering or upgrading mail systems
 - 4) Program managers and information technology (IT) security officers to ensure that adequate security measures have been considered for all phases of the system's life cycle.

2.0 TECHNICAL SPECIFICATION & PRACTICES GUIDELINES

Following features are recommended in the Email Service.

2.1. DOMAIN NAME

The organization should have official email addresses based on single domain name. The email server preferably should be owned by them or government

agency. This gives feeling of unity or belongingness to organization among the employees. The sender should also understand implicit unison of the organization.

The corporate IT department in consultation with chief of communications will establish the domain name to be used in email system.

2.2. **EMAIL SERVICE**

Email services can be web based or client-server based or combination of the two. Any scheme can be considered, but should be adopted enterprise wise uniformly. The Server may be IMAP or POP3. Web based administration for Mail Server should be available. User Authentication may be based on LDAP/ADS. The email system should support distribution list feature with facility for moderator.

All outbound e-mails should have organization's disclaimer at the end. The disclaimer should be jointly developed with the help of legal department.

2.3. **GENERIC/ PERSONAL EMAIL ADDRESS**

In addition to personal email addresses provision for generic email address should be available for specific application eg. Helpdesk, Administrator, COC etc.

2.4. **MAILBOX SIZE**

Each mailbox size should be limited to a default size that should be known to all users. Mail size quota for users must be defined. Maximum mail and attachment size for each mail may also be restricted.

2.5. **MAIL BACK UP**

The Backup of Mail Boxes shall be maintained by the Mail System Administrator as per the approved back up policy. Each mailbox size will be limited to a specified disc space.

2.6. **MAIL BROADCASTING THROUGH BULLETIN BOARD**

(Within the Organization)

The Email Server should have the facility of posting Emails to multiple recipients through Bulletin Board and sharing the address of bulletin board amongst the recipients. This shall be under the purview of Mail System Administrator.

2.7. BROADCASTING POLICY

Grouping of email addresses based on organizational structure is required in most of the organization. The email system should support this. At the same time unauthorized email address should not be allowed to post any information through this channel. This helps to get rid of unwanted Emails for advertisement or any other unofficial purpose.

2.8. RETENTION POLICY OF THE EMAIL IN TRASH

The organization should have retention/ deletion policy for mails in the trash. Such mails may be deleted after certain interval as per the policy. Enterprise should have a uniform and suitable policy on storage and retrieval of mails.

2.9. SECURITY

It should be ensured that the mail Server Operating System & Application is deployed, configured, and managed to meet the security requirements of the organization. Implementation of cryptographic technologies to protect user authentication and email data should be considered.

2.9.1. SECURED NETWORK INFRASTRUCTURE TO PROTECT MAIL SERVER(S).

Email Server along with the network should be adequately secured against hacking & other attacks through layered and diverse protection mechanisms (e.g., firewalls, routers, intrusion detection/protection systems).

2.9.2. PROTECTION AGAINST MALWARE (VIRUSES, WORMS, TROJAN HORSES..)

SPAM control and Anti-Virus protection can be built in the email server. If it is built separately integration of these services with email should be addressed.

Maintaining the security of a Mail Server is an ongoing process. Maintaining a Secure Mail Server requires constant effort, resources, and vigilance from an organization. Securely administering a Mail Server on a daily basis is an essential aspect of mail Server Security. Maintaining the security of a Mail Server will usually involve the following steps:

- 1) Configuring, protecting, and analyzing log files
- 2) Backing up data frequently
- 3) Testing and applying patches in a timely manner
- 4) Testing security periodically

2.10. **RELIABILITY**

Reliability to be ensured through:

- 1) Industry Standard Technology
- 2) Adequate Storage
- 3) High Availability System
- 4) Email Queuing