INTER PLANT STANDARD – STEEL INDUSTRY		
IPSS	**GUIDELINES FOR PC BASED DATA USAGE & SECURITY**	**IPSS:2-08-02-13**

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. Steel Industry has taken rapid strides in leveraging IT for making its business process agile and responsive. It has rolled out various IT applications covering most of the business process. The number of Desktops and Laptops has increased and with people storing most of their data which has necessitated framing guidelines for accessing and securing the desktop and applications.

1. **SCOPE**

1.1. This guideline applies to:
a) All Business PCs
b) Employees using the asset and third party employees maintaining the asset and the IT System provider.

1.2. This guideline shall enable all users of Personal Computer to protect PC based data and use it securely.

2. **OBJECTIVE**

2.1. The objective to be achieved by this guideline is to protect data and maintain privacy of information by ensuring:

1) All stakeholders understand that they should not reveal any data unless expressly authorized to do so.

2) Only the owner of the asset has the right to take decision regarding sharing the data.

3. **PROCEDURE**

The Head of the Dept. will be owner of data stored in the PC used in their department. IT administrator shall be identified for management of Asset & Data.

3.1. The asset should be installed in such a place where risk from following threats are minimized

1) Physical Damage due to Fire, Water, Dust, Heat, Vibration, Accident, theft or terrorist attack
2) Loss of essential services like air-conditioning, power supply
3) Tampering with hardware and software

3.2. Identification of the owner of the asset & maintaining it in a centralized database for the entire organization. Formal handing over of the asset along with all peripherals & software CDs to the asset owner may be carried out through a signed document to be preserved for future reference.

3.3. Ensuring installation & use of only licensed software preferably from a Central Server and under the supervision of a single unit/department. In case of any violation, intimation to be given to the asset owner and/or competent authority so that the incident is not repeated. Awareness to the PC users about consequences of using pirated software as per IT Act.

3.4. Deployment of developed application software shall be done from a central server or by a single agency/department.

3.5. Administrative access of the PC should be with the administrator from IT department. User of the PC will have non-privileged user account.

3.6. Ensuring “Clear Desktop” policy

3.7. Anti-virus software shall be installed as per organization standard. Their shall be regular scanning & updating preferably from a central server

3.8. User will not reveal/share any data and/or information unless he/she is authorized by the competent authority.

3.9. Setting Uniform password policy & awareness across the organization

1) Minimum password length (e.g. 8 characters)
2) Password Expiry Days (e.g. 90 days)
3) Special Characters within password
4) Not to use Date of Birth, Joining, Name of keens, Vehicle Numbers etc. as password
5) Do not use the Remember Password feature on any application.

3.10. Before using removable media its source and authenticity must be ensured. Removable media from only authentic & trusted source to be entertained for data exchange. It is to be ensured that virus scan shall be done before using removable media. The data exchanges via removable media should be recorded & records are to be maintained for a defined time period decided by the competent authority.

3.11. Regular backup of the PC is the responsibility of the asset owner. The owner may however identify critical data & store it at a central server which will be backed up as per central backup policy. The IT department should provide facility for such backup.

3.12. Before shifting the asset from one owner to the other, handing over for maintenance or disposal, it must be ensured that no sensitive data go along with the asset. Either backup the partitions having user data/files and format or format the entire PC and install OS only before handing over.

3.13. All incidents violating the guidelines to be reported, investigated and further steps to be taken. It shall be properly documented to prevent its reoccurrence.

3.14. The organization shall have right to access all the data on any PC provided by the organization. However the owner of the PC shall be responsible for the data & programs.

4. Responsibilities

4.1. Asset owner’s responsible for awareness of the policy to the asset users.

4.2. All stake holders should adhere to the policy.