1. Information Security Measures

The issue of metadata and hidden information exposure when transferring information through formats like Microsoft word, excel and power point is very high. For comprehensive content and information security, content filtering and metadata/hidden information inspection shall be deployed.
Some of the main points considered to ensure that there is no leakage when transferring data through the above-mentioned formats includes:

1. Wherever possible, Microsoft word, excel and power point files should be converted to pdf files before sending to any third-party user including customers, potential customers etc)
2. Incase Microsoft excel has to be sent, ensure that filtered rows, comments, hidden fields, unwanted or hidden sheets, unwanted header-footer information, macros are not present
3. In Power Point has to be sent, ensure that hidden slides, unwanted information in notes, comments are not present
4. In case of Word has to be sent, ensure that Comments and History of changes are not present
5. In case of Microsoft Word, Excel or PowerPoint, cross check the information contained in File->Properties->Summary, and make sure it is relevant
6. While preparing any documents in a template, always take the document template using File -> New than reusing another document of the same template.

Details regarding implementation of the above-mentioned points are given below

1.1 Converting to PDF

Usage of pdf provides the advantage that all the information to be presented is directly seen-there will not be any metadata. Also, the files can be made read only thus preventing editing.

i. **Creation of PDF**

Select the File tab.

Select **Save As.**

To see the **Save As** dialog box in, you have to choose a location and folder.

In the **File Name** box, enter a name for the file, if you haven't already.

In the **Save as type** list, select **PDF (*.pdf)** .

1.2 Security Measures

II. **Security Level**

Set the security level to medium or higher. This measure will notify you by a dialogue box of any unsigned macros and will let you disable such macros.

- On the **Tools** menu, point to **Macro**, and then click **Security**

- Click the **Security Level** tab, and then select the security level you want to use (This should not be lower than medium)

III. **Read Only**

- Open the document.
- On the **File** menu, click **Save As**.
- On the **Tools** menu in the **Save As** dialog box, click **General Options**.
- Select the **Read-only recommended** check box, and then click **OK**.
- Click **Save**.

IV. **Password Security**

- Open the document.
- On the **File** menu, click **Save As**.
- On the **Tools** menu in the **Save As** dialog box, click **General Options**.
- In the **Password to Open/ Password to modify** box, type a password, and then click **OK**.
- In the **Re-enter Password to Open/ Password to modify** box, type the password again, and then click **OK**.
- Click **Save**

V. **File Properties**

- Update Properties of file to make sure no proprietary information is displayed
- On the **File** menu, click **Properties**, and then click the **Summary** tab.
- Type any information you want in the file properties boxes

VI. **Removing Unwanted Macros**

Additional macros that are not needed for the document, at times, could be linked with the same. To remove unwanted or unintended macros from a document,

- Open the **workbook** that contains the macro you want to delete.
- On the **Tools** menu, point to **Macro**, and then click **Macros**.
- In the **Macros in** list, click **This Workbook**.
- In the **Macro** name box, click the name of the macro that you want to delete.
- Click **Delete**

1.3 Security measures for Excel

In case Microsoft excel must be sent, ensure that filtered rows, comments, hidden fields, unwanted or hidden sheets, unwanted header-footer information, macros are not present. This has the potential risk that filtered rows, comments, hidden fields, unwanted or hidden sheets, unwanted header-footer information, macros, which are not expected to be seen by the third party, remain hidden because of the filtering.

i. **Filtered Rows**

Use the option **Data**->**Filter**->**Show All** to display all rows in a filtered sheet and check if any unintended information is present in the sheet

ii. **Comments**

To delete all comments, right click between **Column A** and **Row 1**(this will select full sheet) and give option **Delete Comment**

iii. **Hidden cells**

To display all hidden cells, right click between **Column A** and **Row 1**(this will select full sheet). Point to **Row** or **Column** on the **Format** menu, and then click **Unhide**.

iv. **Unwanted/Hidden Sheets**

To display any hidden sheets, point to **Sheet** on the **Format** menu. Select the hidden sheet name that you want to view, and then click **OK**.

v. **Unwanted header-footer information**

To view whether any header footer information is set, go to **Header and Footer** in **View** menu. Verify whether the information provided in the **Header** and **Footer** boxes are valid. If header / footer information is not needed, change the **Header** and **Footer** combo in the same, to **none**.

vi. **Embedded excel files**

In case where excel files or part of excel files need to be embedded in a word or power point, it is possible to retrieve the entire data on the embedded excel file by double clicking the object. To avoid the risk of unwanted information being leaked out from embedded excel file,

- Copy all the excel information to be embedded
- Use **Paste Special**->**Format** and then **Paste Special**->**Values** to paste the information only into a new excel file.
- Copy from the new excel file to embed the excel sheet in word or power points

vii. **Workbook protection**

Protect workbook/ worksheet in-case the intender need not change any of the contents of the excel.

- On the **Tools** menu, point to **Protection**, and then click **Protect Sheet**.
- To prevent others from removing worksheet protection, type a password, click **OK**, and then retype the password in the Confirm **Password** dialog box. Passwords are case sensitive.

To provide permission to access specific areas of a protected worksheet unlock the ranges that you want users to be able to change or enter data in.

- Before protecting the sheet, select the cells that you want to edit even after protection.
- On the **Format** menu, click on **Cells**.
- From the **Protection** tab of the **Format Cells** dialog box, uncheck the **Locked** option.

1.4 Security Measures for PowerPoint

i. Hidden Slides

The PowerPoint hidden slide feature (**Slide Show** > **Hide Slide**) allows individual slides to be hidden during the slide show and printing of the presentation. Hidden slides may contain information that is not intended for release.
It is recommended that presentations that contains hidden slides should be reviewed prior to distribution to determine whether the hidden slide(s) should be removed

ii. Presentation Notes

The PowerPoint notes feature allows notes to be associated with each slide. Notes may contain general content or internal commentary that should be reviewed or removed prior to distributing a presentation.
It is recommended that ppresentations should be inspected for Presentation Notes prior to distribution, allowing authors or administrators to determine whether such notes are appropriate for third party exposure

1.5 Security Measures for Word

i. Versions

Remove all other versions of the document stored in the file

- On the **File** menu, click **Versions**
- Click the version of the document you want to delete
- To select more than one version, hold down **CTRL** as you click each version
- Click **Delete**

ii. Track changes

Disable track changes before sending any document.

iii. Usage of Wordpad

If a Word document received by e-mail seems suspect, it is preferable to open it with Wordpad rather than with Word, because *Wordpad* does not recognize and will not open macros