Data Classification Guidelines in Power BI

Last updated by | Teruyuki Ito | 7 Oct 2024 at 08:38 BST

Key people

- Teruyuki Ito - Reporting and Data Visualisation manager (FT)

In Power BI, data classification refers to the practice of categorizing and labelling data based on its sensitivity or confidentiality level. On top of complying on the ISO standards, this feature helps us in protecting our data by ensuring that our stakeholders and clients are aware of the nature and appropriate use of the data they are interacting with.

Power BI integrates with Microsoft Information Protection (MIP) to apply sensitivity labels to datasets, reports, dashboards, and dataflows. These labels help indicate how sensitive or confidential the data is and inform us about how the data should be handled. Sensitivity labels are defined and managed by Maximus Information Security department through Microsoft 365 compliance policies.

The Maximus classifications are as follows;

- Official / Sensitive - Information, which if disclosed without authority (even within the organisation) would cause serious damage in terms of financial loss, legal action, or loss of reputation. Access is restricted to personnel with specific roles and clearance or with statutory rights of access.

  Examples are;
  • Special Category Data, e.g., health or disability records
  • Financial payment information, e.g., bank account information
  • Business Continuity Plans (containing staff emergency contact details)
  • Investigation evidence
  • Commercially sensitive information

- Official -Information available to approved individuals within Maximus UK and which contains business value, or which requires protection due to it being personal or confidential data. Access is restricted to staff within the organisation in connection with their employment.

  Examples are;
  • Procedures
  • Business Continuity Plans (without staff contact details)
  • Emails or customer records (other than that containing Official-Sensitive data)
  • IT Procedures relating to the Data Centres, Network, Backups etc.
  • Personnel files (unless they contain health or disability information)
  • Contracts
  • Draft service plans
  • Restructuring documentation

- Public - Information that can be made available in the public domain and which would not cause damage or harm if released.

  Examples are;
  • Policies
  • Office opening times.
  • Business phone numbers.
  • Press releases.
  • Forms.

• Some Statistics and Performance Indicators.
• General recruitment information, and terms and conditions of employment

All reports, dashboards, dataflows and apps that is created in DnA has to be data classified. This can be done in 3 ways;

1. Assigning a sensitivity label at the report settings in the workspace.
2. Assigning a sensitivity label on the Power BI desktop
3. Assigning a sensitivity label at the semantic model in the workspace.

The last one is the most preferred since setting the right label to the semantic model will propagate out the label downstream.

Once applied, sensitivity labels are visible to our stakeholders and clients who interact with the content in Power BI, such as when viewing a report or dataset. This ensures that they will be aware of the level of sensitivity of the data and the need for caution when sharing or using the data.

Currently, we have automatically set the label to "Official" as a default label configured in the admin portal. Our BI developer can still manually select a different label as needed by following either of the 3 ways describe above.

On top of that sensitivity labels in Power BI are not just for informational purposes, they can also trigger automated security policies. For example:

- Preventing unauthorized sharing of sensitive data.
- Applying encryption to reports or datasets that are classified as confidential.
- Limiting export, sharing, or printing of highly sensitive data.
- Consistency Across Microsoft 365 Ecosystem, Power BI’s data classification and sensitivity labels are integrated with the broader Microsoft Information Protection (MIP) framework, which allows our information security department in Central to apply the same labels and policies to data in other services, such as Excel, SharePoint, and Outlook. This ensures consistent data governance across Maximus.

Data classification in Power BI, particularly through the use of sensitivity labels, is a way to categorize data based on its sensitivity and ensure that appropriate security measures and handling policies are followed. This system allows Maximus to better protect sensitive information, maintain compliance, and enforce governance policies across their data ecosystem.