Australian Government

Industry Data Classification Framework

The Industry Data Classification Framework (IDCF) is a voluntary tool for organisations to classify data, identify controls to protect it and communicate the required protection to others in accordance with a code of conduct. The IDCF consists of three core elements that organisations can use flexibly based on their specific business needs.

	Risk assessment	Data Security Levels (DSLs)	Markers
Included in framework	• Simple, practical method to assess risks and potential consequences associated with data holdings • Assessment tools, including guidance on adverse events and impact • Examples of physical, cyber and authorised-person threats	• Simple classification system based on the use of labels • Common language to communicate required level of confidentiality, integrity and availability • Rules for classification, storage and reclassification • System configuration guidance aligned to maturity models • Access control and user-management expectations	• Optional secondary classification system to be used alongside DSLs to communicate additional context about data handling • Marker categories and how to use them • Guidance on consistent naming conventions • Guidance on effective use of markers when sharing data internally and with partners
Benefits	• Provides a clear, standardised approach to assessing data risk • Improves data literacy and confidence in risk decisions • Helps organisations prepare for adverse cyber, physical and insider events	• Provides a common, shared classification language • Aligns with existing standards (such as Protective Security Policy Framework, Australian Signals Directorate's Essential Eight) • Reduces likelihood of compromise by matching data to proper controls • Provides clear requirements for data-sharing	• Adds contextual information to DSLs (e.g. privacy, cultural, legal) • Improves internal governance with clearer handling and access expectations • Aligns with existing internal processes and external schemes (such as the Traffic Light Protocol) • Builds trust in data-sharing by clarifying expectations and restrictions
Workflow	**Step 1: Assess risk** Organisations identify their data holdings and consider the potential consequences, impact and likelihood of adverse events. E.g. An organisation determines a *Project Update* requires a high level of protection against most threats.	**Step 2: Classify data** Organisations label the data with the appropriate DSL based on the required protection. E.g. An email with the following subject line: *Q3 Project Update: DSL-3*	**Step 3: Apply optional markers** Organisations may choose to add markers to the DSL label to communicate additional information. E.g. A document with the following in the header: *Q3 Project Update: DSL-3, Cultural*