

ISO/IEC TS 38505-3:2021-12 (E)

Information technology - Governance of data - Part 3: Guidelines for data classification

Contents		Page
	Foreword	v
	Introduction	vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Foundations	4
4.1	Context.....	4
4.1.1	The data deluge.....	4
4.1.2	The strategic value of data.....	4
4.1.3	The risks associated with data.....	4
4.1.4	Consequences of failure.....	4
4.2	Data classification.....	5
4.3	Purpose of classification.....	5
4.4	Engage and empower staff.....	6
4.5	Structure of this document.....	6
5	Roles and responsibilities	6
5.1	General.....	6
5.2	Role of governing body.....	8
5.2.1	General.....	8
5.2.2	Understanding the role of data.....	8
5.2.3	Governance of data.....	8
5.2.4	Data classification approach.....	8
5.2.5	Data classification and risk management.....	8
5.2.6	Direct according to policy.....	9
5.2.7	Monitor conformance and performance.....	9
5.3	Role of management.....	9
5.3.1	General.....	9
5.3.2	Setting the scope of data classification.....	9
5.3.3	Propagating and implementing policy.....	9
5.3.4	Defining roles and responsibilities.....	10
5.3.5	Mobilizing the organization in support of the policy.....	10
5.3.6	Operation.....	11
5.3.7	Feedback from management to the governing body.....	11
5.3.8	Levels, discovery and attribution.....	11
5.4	Changing classifications.....	11
5.5	Defining the requirements: key considerations.....	12
6	Data classification framework	12
6.1	Context.....	12
6.2	Identification.....	13
6.3	Implementation.....	13
6.4	Monitor/Improve.....	14
7	Guiding principles	14
7.1	Simplicity.....	14
7.2	Default classifications.....	14
7.3	Interoperability.....	14
7.4	Equivalence.....	14
7.5	Use of data classification for processor and controller.....	15

7.6	Auditing, controls and compliance.....	15
7.7	Customer data.....	15
7.8	Assessment and reporting.....	16
7.9	Learning, maintaining and improving.....	16
7.10	Data protection.....	16
Bibliography		17