Classification of documented information

Last updated by: QA Elin Lindblom
Date: 2023-06-14

According to *A.8.2* in **ISO/IEC 27001:2017** (and *A.5.12-13* in **ISO/IEC 27001:2022**) information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
The information is also to be classified according to the information security needs of Awave based on confidentiality, integrity, availability (abbreviated C.I.A.) and relevant interested party requirements.

What this means in practice is that Awave has listed all relevant documented information, and classified it accordingly. The C.I.A. is considered, and any safety aspects of the asset.

In short, it's about how valuable the information is to Awave, and what level of protection is needed.

Explanation of classifications:			
A=serious	B=considerable	C=moderate	D=none or negligible