21.4. Databases

Objective

21.4.1. Database content is protected from personnel without a need-to-know.

Context

Scope

21.4.2. This section covers information relating to databases and interfaces to databases such as search engines.

Rationale & Controls

Data labelling

21.4.3.R.01. **Rationale**

Protective markings can be applied to records, tables or to the database as a whole, depending on structure and use. Query results will often need a protective marking to reflect the aggregate of the information retrieved.

21.4.3.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:4434]

Agencies MUST ensure that all classified information stored within a database is associated with an appropriate protective marking if the information:

- could be exported to a different system; or
- contains differing classifications or different handling requirements.

21.4.3.C.02. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:4435]

Agencies MUST ensure that protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any classified information retrieved or exported from a database.

21.4.3.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4436]

Agencies SHOULD ensure that all classified information stored within a database is associated with an appropriate protective marking if the information:

- could be exported to a different system; or
- contains differing classifications or different handling requirements.

21.4.3.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4437]

Agencies SHOULD ensure that protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any classified information retrieved or exported from a database.

Database files

21.4.4.R.01. **Rationale**

Even though a database may provide access controls to stored data, the database files themselves MUST also be protected.

21.4.4.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:4440]

Agencies MUST protect database files from access that bypasses the database's normal access controls.

21.4.4.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4441]

Agencies SHOULD protect database files from access that bypass normal access controls.

Accountability

21.4.5.R.01. **Rationale**

If system users' interactions with databases are not logged and audited, agencies will not be able to appropriately investigate any misuse or compromise of database content.

21.4.5.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:4444]

Agencies MUST enable logging and auditing of system users' actions.

21.4.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4445]

Agencies SHOULD ensure that databases provide functionality to allow for auditing of system users' actions.

Search engines

21.4.6.R.01. **Rationale**

Even if a search engine restricts viewing of classified information that a system user does not have sufficient security clearances to access, the associated metadata can contain information above the security clearances of the system user. In such cases, restricting access to, or sanitising, this metadata effectively controls the possible release of information the system user is not cleared to view.

21.4.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4448]

If results from database queries cannot be appropriately filtered, agencies MUST ensure that all query results are appropriately sanitised to meet the minimum security clearances of system users.

21.4.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4449]

Agencies SHOULD ensure that system users who do not have sufficient security clearances to view database contents cannot see or interrogate associated metadata in a list of results from a search engine query.