JSP 602 Instruction	1007	**Applicability**	Applications, Infrastructure
Configuration Identity	Version: 01.02 Amended: 2009-01-18 Reviewed: 2009-01-18	**Epoch Applicability**	2008 - 2011

JSP 602: 1007 - Database Services

Outline

Description: Database Services are the protocols and standards required to create, manage and replicate a database and the languages and schema required to allow systems and services access to the information contained within the database.

Reasons for Implementation: The purpose of this policy is to inform developers how to create and manage databases and to provide MOD CIS with the means required to allow them to access information contained within these databases. These services provide access to data independently of the process that created it and provide the means to define and share data in a timely and accurate way across processes and platforms and therefore provide data interoperability among GII systems and services.

Issues: Databases are important information repositories and will exist across the GII. Sophisticated protocols are employed within commercial and bespoke products to perform functions such as transaction management and selective attribute-based replication. In order to access information within a database it is essential that details of the schema, access methods and data dictionary are published and that a standard query language is supported.

Guidance: This policy is outside the scope of the e-GIF.

This policy is consistent with the NC3TA.

Policy

Strategic

1007.01: Database Access
 	
1007.01.01 All systems and/or projects providing database(s) or accessing databases shall do so using the following standards:
 	
    1007.01.01.01 SQL 3 Full Level (ISO/IEC 9075:1999)
 	
    SQL is a standard programming language for getting information from, and updating to, a database. It has widespread commercial support with many database products supporting SQL through the addition of proprietary extensions to the standard language.
 	
    Comment: SQL queries take the form of a command language that lets you select, insert, update, find out the location of data, and so forth. There is also a programming interface.
 	
1007.02: Database Time Synchronisation
 	
1007.02.01 The mandated policy for the time synchronisation of databases is contained in JSP602: 1027 - Time Services.
 	
Comment: Distributed databases must use a common time reference and thus require a standard time source. Network time synchronisation is achieved through the use of NTP.
 	
1007.03: C2 Information Exchange Data Model
 	
1007.03.01 All systems and/or projects exchanging C2 information within and interoperating with the Land Environment shall as a minimum support the following standard. It is strongly recommended for other Environments:
 	
    1007.03.01.01 JC3IEDM, NATO STANAG 5525
 	
    The common data interchange specification of NATO.
 	
    Comment: The exchange of C2 information requires the implementation of a physical instance that is compliant with, or can be mapped to, the JC3IEDM, STANAG 5525 and MIP Baseline documentation (including all MIP business and implementation rules).
 	
1007.04: Database Replication
 	
1007.04.01 Nothing is mandated at this time (see comment).
 	
Comment: There are no open and widely supported standards for database replication, consequently each specific DBMS implements a proprietary replication mechanism that uses a format only readable by itself. Where database replication is required MOD projects must adopt a common product. Replication draws its primary benefit from an ability to balance load on a network by replicating frequently accessed database records at specific geographical locations (and thus reducing network traffic). Replication is not appropriate where data consistency must be maintained at all times and updates of data records require immediate dissemination.
 	
1007.05: Schema, access methods and data dictionary
 	
1007.05.01 All systems and/or projects providing database(s) shall publish the schema, access methods and data dictionary for each database they provide.
 	
To allow other systems/services to access a database the schema, access methods and data dictionary must

be published and made accessible to application developers.

Strategic (continued)
1007.05.02 Schema and data definitions shall comply with MOD data management policy contained within JSP602: 1008 - Defence Data.

Deployed
As for Strategic domain.

Tactical

1007.06: Database Access
1007.06.01 Nothing is mandated at this time, however it is highly recommended that where infrastructure constraints permit, the 'Strategic' policy should be followed.
 	
Comment: Database access is likely to be prohibited because of bandwidth and security constraints. However where databases need to be shared within a local area such as a Tactical HQ then SQL 3 should be used.
 	
1007.07: Database Time Synchronisation
As for Strategic domain.
 	
1007.08: C2 Information Exchange Data Model
1007.08.01 All systems and/or projects exchanging C2 information shall as a minimum support the following standard:
 	
    1007.08.01.01 JC3IEDM, NATO STANAG 5525
 	
    The common data interchange specification of NATO.
 	
1007.09: Schema, access methods and data dictionary
As for Strategic domain.

Remote
Not applicable.

Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all MOD Projects (and their suppliers) that provide and use database services.

Procedure

Not Applicable.

Relevant Links

JSP602: 1005 – Collaboration Services

JSP602: 1027 - Time Services

JSP602: 1008 - Defence Data

ISO standards can be purchased from the ISO web site here.
(http://www.iso.org/iso/en/CatalogueListPage.CatalogueList)

A glossary of terms and abbreviations used within this document is available here.

Instructions on how to read a JSP602 leaflet are available here.

Compliance

Stage	Compliance Requirements
Initial Gate/DP1	MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s).
Main Gate/DP2	MOD Projects shall reference in their SRD (and MODAF technical views) the specific policy elements contained within this leaflet that are applicable to the infrastructure they are procuring or updating.
Release Authority/DP5	MOD Projects (supported by their equipment suppliers) shall provide evidence of their compliance with the elements of this policy defined within the SRD (and MODAF technical views). Evidence of conformance with standards shall be presented; sources of evidence may include: conformance/compliance certificates provided by equipment suppliers (e.g. under type approval or other assessment regimes), demonstrations, inspection, analysis, tests carried out by suppliers (e.g. Factory Acceptance Tests) and tests carried out at Defence Test and Reference Facilities.