



# GDOT Publications

## Policies & Procedures

---

**Policy:** 8075-3- Database System Access Standard  
**Section:** Database Standards  
**Office/Department:** Office of IT Application Support & Development

**Reports To:** Division of Information Technology  
**Contact:** 404-631-1000

### PURPOSE

The purpose of this standard is to establish common, standards-based database conventions. It identifies database types, access languages, protocols, and connectivity methods that enable database access. This helps to reduce total cost of ownership while increasing efficiencies in data sharing, data security and database support.

### SCOPE

1. This policy applies to all GDOT IT personnel (including employees, consultants, contractors, vendors and other third parties) actively engaged in database design, development, or modification; and to any outside entities engaged in developing IT applications for GDOT.
2. This standard is applicable to database technology, both independent and contained in software application systems, utilized by GDOT with the exception of personal use databases contained in office productivity software and solutions.
3. Exception to this standard must be approved by the Administrator of IT Applications.

### RESPONSIBILITY

1. The Administrator of the Office of IT Applications is responsible for compliance with the standard, updates to the standard, and enforcing the standard.
2. GDOT IT Team Leaders are responsible for compliance with the standard and for reporting concerns to the IT Application Administrator.

### DEFINITIONS

This standard recognizes that different types of database technology and database management systems (DBMS) exist. For the purposes of this standard, types of database technologies included are:

1. Relational, including object-relational
2. Object-oriented
3. Other, including native Extensible Markup Language (XML) database Technology and Vendor applications that use "Black Box" or custom developed database engines

## STANDARDS

1. All IT developed databases shall operate and be implemented on GDOT supported databases platforms and versions/patch levels.
2. Database implementation, management and access shall be securely implemented with regard for availability, integrity, and confidentiality of the data as established in GDOT Information Security Policies.
3. Database technologies shall comply with GDOT approved ANSI, ANSI/ISO/IEC, and ISO/IEC standards.
4. Structured Query Language (SQL) implementations within database technology shall comply with GDOT approved ANSI, ANSI/ISO/IEC, and ISO/IEC standards. Proprietary, vendor-specific, SQL extensions may limit flexibility and adaptability and are not recommended for general use.
5. Database technologies shall provide the capability for the following types of connectivity:
  - Java Database Connectivity (JDBC) providing the application program interfaces (API) to connect Java programs to a wide range of cross-DBMS SQL databases.
  - Open Database Connectivity (ODBC) providing the API promoting open connectivity to various databases.
6. The entry and update of data stored in GDOT and GDOT databases shall be accomplished in accordance with the business rules established in software application systems.
  - Data shall be entered and updated using software applications and business rules to protect the data from unauthorized or accidental access, and to ensure security, data integrity, and accurate interpretation of the data.
  - Data access and permissions shall be assigned within the context of the software application, and shall be in accordance with the GDOT Information Security policies.
  - 'Read' access to view GDOT's data shall be provided through established ad hoc enterprise reporting applications such as (SAP) Business Objects/Web Intelligence or the Geographic Information System (Esri ArcGIS).
7. Free-form data entry and update using direct database access shall be restricted.
  - Direct database access, when required, shall require the IT Application Administrator's approval. Business steward of the data shall provide written delegated authority or specific access permissions in accordance with the GDOT Information Security policies, and are responsible for ensuring that the relevant business rules implemented by the software application system for normal entry and update are not violated.
  - Under special circumstances mandated by the project and for a finite amount of time, with the approval of the IT Applications Administrator, read-only direct database access for ad-hoc querying and reporting, or location mapping may be allowed.
8. Database technologies shall reuse GDOT's common security and access control mechanisms to ensure interoperability and compatibility with network and platform operating systems, as well as software application security.
9. Database access routines should be written to be independent of the platform and underlying data structure.
10. GDOT shall implement access control measures within database systems for identifiable authorized individuals. Database implementations shall electronically and automatically capture sufficient identifying user information to know every user's sessions (except public access users) for a period of time to be determined by the GDOT's security personnel. Factors such

as level of access (read only vs. edit), data sensitivity classification, etc. shall be taken into consideration in determining user login archiving.

11. User access to data shall be terminated immediately upon separation from GDOT or a change in job responsibilities that no longer make the access appropriate.

**References:**

None.

**History:**

requirements for the Geographic Information System incorporated: 11/05/12

copied to GDOT Publications v.02.00.00: 02/29/12;

reviewed: 7/6/2010;

copied to P&P: 10/01/09;

created and made effective 09/01/09