DB Password Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose
This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of <Company Name>'s networks.

Computer programs running on <Company Name>'s networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

2.0 Scope
This policy applies to all software that will access a <Company Name>, multi-user production database.

3.0 Policy

3.1 General
In order to maintain the security of <Company Name>'s internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

3.2 Specific Requirements

3.2.1. Storage of Data Base User Names and Passwords
- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

3.2.2. Retrieval of Database User Names and Passwords
- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

- For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

3. Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

4. Coding Techniques for implementing this policy

[Add references to your site-specific guidelines for the different coding languages such as Perl, JAVA, C and/or Cpro.]

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Computer language	A language used to generate programs.
Credentials	Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.
Executing body	The series of computer instructions that the computer executes to run a program.
Hash	An algorithmically generated number that identifies a datum or its location.
LDAP	Lightweight Directory Access Protocol, a set of protocols for accessing information directories.
Module	A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.
Name space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.
Production	Software that is being used for a purpose other than when software is being implemented or tested.

6.0 Revision History