Database Security Technical Document

It is recommended that if a casino employees, consultants, or corporate staff directly accesses a database that contains regulated gaming data for business purposes the account they use should be restricted to read only permissions. Direct access means any method of accessing a database that circumvents the vendor's application, or approved access method such as a gateway.

Accessing the gaming system database with an account with read only/view privileges still represents a risk to the availability of the system as well as data integrity. The Division recommends that the casino test any batch procedures including queries, scripts or reports built in 3rd party tools such as Crystal Reports in a test environment prior to implementation in the production environment. It is recommended that the casino also request the gaming system manufacturer review the batch procedures, to ascertain if the procedures will negatively affect the system. The casino should have formal written processes and procedures documenting (i.e. project plan) the development and testing of any code that is not included with the gaming system. Software should be made available to the Division upon request.

Licensed technicians from the software vendor or licensed 3rd party consultants may use a unique account with elevated privileges along with tools and methods approved by their company to complete maintenance or repairs. These tools and methods can include, but are not limited to 3rd party software packages, direct edits, or scripts. The casino must complete the RAMP log for any maintenance, repairs or upgrades affecting the gaming system. .

Examples of accounts with elevated permissions that should be limited to IT include:
(The following is not a definitive list of accounts it represents an example of common accounts used to modify the database environment or the data contained within it.)

- The default database System Administrator(SA) account
- System accounts installed with a software package
- System accounts that enable communication with the database such as an ODBC connector.
- Database administrator accounts assigned to casino employees within the IT department.
- Vendor accounts for support

Examples of commands that an account with elevated rights can execute might include:
(The following is not a definitive list of commands it represents a list of common commands used to modify the database environment or the data contained within it.)

Modifications to data using commands from the Data Manipulation Language (DML) such as:
UPDATE, DELETE, INSERT INTO statements
Modifications to tables, indexes, links or constraints using the Data Definition Language (DDL) such as:
CREATE, DROP or ALTER Database
CREATE, ADD, DROP or ALTER table
CREATE, or DROP index

Accounts with elevated permissions in the database environment must be unique for each user and must not be shared between the casino's employees. Passwords for system accounts that allow software packages access to the database and have the ability to modify the database or objects within the database must never be given out and the accounts must only be used by the system and never by a casino employee in lieu of their personal account. System accounts must always have their default password changed.

For more information on password management please refer to the Logical Security document.

Third party tools like Crystal Reports or other software tools packaged with the gaming systems including supporting systems (such as Microsoft's Server Enterprise Manager) can be used by accounts that have **read only rights** and are limited to query (view only) access. 3rd party tools are defined as any software product or batch procedure that is not developed by the gaming system's manufacturer. This includes software or batch procedures that are developed in house, as well as software from other vendors or contractors.

If the casino is not using the gaming system's gateway it must submit must request a variance and receive acknowledgement from the Division prior to use. If the casino currently has software packages not using the gateway, send an email to either dor_ccbhcasinos@state.co.us or dor_cripplecreekcasinos@state.co.us with the name of the application and a brief description.

Even with read only permissions, batch procedures such as queries or scripts with generic database calls can disrupt the system and in some circumstance cause data loss. Best practices, such as explicitly coded table names should be maintained. For example read only ad-hoc queries should be written in a way that will not jeopardize the production environment if it locks the database or runs long. Please contact the gaming system vendor for best practices regarding their system.

All documentation must meet the requirements in the documentation section.

1.4b, 1.6b
The Division recommends that all modifications and access to the database be logged by the system and reviewed by the casino. This includes but is not limited to:

- Any action taken by an account with elevated privileges
- Invalid Login attempts
- Initialization of audit logs
- Creation and deletion of system level objects

System generated logs should include the following information:

- Time/Date stamp for each entry
- User Identification
- The Type of event
- Event ID
- Success or Failure (If applicable)

Time/Date stamps should be validated using a time synchronization system such as a Network Time Protocol (NTP) server and the time/date stamps should be protected.

Please note the following pertains to system disruptions.

Unanticipated incidents

System Disruption

When an unanticipated incident occurs that causes a disruption in the collection, accuracy, integrity, or availability of the gaming system, the casino must immediately contact the appropriate IT resources to begin the troubleshooting process. The casino must add an entry to the RAMP log, and inform the Division as soon as practically possible via e-mail. The e-mail must include, but is not limited to, a detailed description of the problem, why they think the problem occurred, if the manufacturer was contacted to assist in or to resolve the issue and if not, why not, the time it was identified, a brief statement about where the casino/vendor is in the troubleshooting process and the manufacturer's case number (if applicable).

The Division does not require that the casino waits for an acknowledgement from the Division before proceeding with the solution.

After the problem has been resolved, a follow up email must be sent to the Division within 48 hours of resuming normal operations. The email must include a description of and resolution to the problem.

This applies to both an incident where as a result of manipulating the database directly with an account that has elevated privileges a disruption has occurred or as a result of the system failing it becomes necessary to directly access the database with an account that has elevated privileges to affect a repair.

The documentation can be submitted to the Division via email.

Exceptions

Incremental maintenance to the Operating System (***OS)*** or the Database (***DB)*** such as installing:

- Patches (OS/DB)
- Updates (OS/DB)
- Hot fixes (OS/DB)
- Service Packs (OS/DB)
- Service Releases (OS/DB)
- Maintenance release (OS/DB)

Software upgrades and updates as outlined in the ICMPs must be submitted to the Division via email on the required Notification of Intent to Install/Upgrade form located on the Division's website.

All references to providing the Division with documentation should be emailed to the addressed stated in the General subsection of this section.