Logical Security Technical Document

Logical Security is part of an in-depth defense strategy that includes account and password management, managing default settings and installing security software that can help mitigate risk. It requires evolving solutions as new threats emerge and new technologies become the standard.

Account management can be broken down into user accounts, accounts that are assigned to a single user. System accounts, these accounts are used by the system for connectivity such as an application's access to a database. Generic accounts, which are shared by multiple users can represent an efficient solution: however, due to the risk involved, most are not allowed.

Some examples of allowed generic accounts:

- Meter card
- Jackpot fill

Examples of disallowed generic accounts:

- Count Team
- Marketing User
- Slot A
- Test

User accounts are accounts specifically assigned to a single user. They are built on the principle of least privilege and require ongoing review to ensure that the account is appropriate to the user's job. These accounts should be approved by the employee's manager before access is granted. Refer to the SOD documentation for management approval requirements. The account must be deleted or disabled within 3 days of the employee's last shift. Refer to the Employee Confirmation and Termination documentation.

System accounts must only be used for the purpose in which they are built and must never be used by an employee in lieu of their user account. Some system accounts can be included by default in a software package. These accounts must always have their passwords changed prior to the system going live. In addition to having the default password changed, system accounts must have their passwords changed when a person with knowledge of the password(s) leaves the company. System passwords have additional management considerations such as passwords being documented and the document stored in a secure area. Password change requirements for system accounts with minimum risk or access rights may be exempted upon Division review.

Examples of system accounts include but are not limited to:

- Currency card
- Meter card
- Jackpot fill
- Kiosk
- ODBC Connectors

Both user accounts and system accounts can have elevated privileges. Accounts with elevated privileges should be limited to IT for administrative functions. All accounts with elevated privileges must have their passwords changed at least annually. They must also be changed whenever a person with knowledge of the password(s) leaves the company. All accounts with elevated privileges must be approved by management and reviewed annually.

Database Account Management

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 an individual in lieu of their personal account. System accounts must always have their default password changed.

3rd 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. Refer to the database ICMP for more information.

Wireless Account Management

The following sections clarify the wireless ICMP:

Account Management:

- Using strong pass phrases – Strong pass phrases should include letters, numbers and special characters. The pass phrases should be no shorter than 8 characters, but 13 characters are recommended.
- Changing default passwords – There are typically one or more accounts that are established by default from the manufacturer. The most common is an administrator account. Passwords must be changed before the wireless device is implemented.

- Minimize the number of people who have access to accounts with elevated privileges.
- Accounts with elevated privileges must have their passwords change at intervals no longer than 90 days.
- The authentication routine should be encrypted.
- The change should be documented and reviewed by management.
- Devices or accounts that timeout must authenticated again.

Password Management includes password complexity, length, history, interval of change. Passwords should be a minimum of 8 characters. The selection of characters should include numbers and special characters. Letters must have the option of upper and lower case. The system should be configured to not allow the same password within 4 password change intervals. Passwords should be changed at least every 90 days. Default settings are typically a selection of settings configured by the manufacturer to enable the easiest use of their product. These settings are not usually the most secure. Defaults such as passwords and SNMP community strings should be changed before the device is put into a production environment. Services, features, and protocols that are not being used by the casino should be disabled. Log retention should be adjusted to meet the requirements of the casino and the Division. Accounts that are members of default groups that are not being used should be removed. If the account is not being used it must be removed or disabled.

Wireless Default Settings

Parameters that should be changed include but are not limited to:

- Default Pre-shared key (1.2a)
- SSID (1.2b)
- SNMP community strings (1.2c)
- Encryption Keys (1.2d)
- Passwords (1.2E)
- Disable any unnecessary ports, protocols, broad casts or other options (1.2f)
- Change clock settings to synchronize with the casino's time system (1.2g)
- Set a session timeout (to prevent hijacking of abandoned authentication sessions(1.2h)

Disable WPS (1.2i)

Changes to the default settings should be documented.

Security software should be updated on a regular basis and configured to monitor the server on which it is installed. It should also be configured to scan the server at a regular interval and notify an administrator or responsible person of any potential threats. Programs such as anti-viruses and anti-malware should be configured to update at a minimum once per day.