|  |
| --- |
| Home Start Realty |
| MEMO – Internal, Confidential |

To: Brendan McAlister

From: Chad Ballay

Subject: Database Audit and Security Review

This will serve as a rough guideline for addressing the Audit and Security needs as per the database administrators purvey. This document should be considered advisory and a living document.

# Classification

Which type of audit are we aiming to accomplish will dictate the posture and processes executed in subsequent steps. Deciding and then clearly stating the type of audit will allow for the work to progress at pace. Informal, Formal Internal, External, and Automated are common classifications but that is not an exhaustive list.

# Goal

The enumerated list of goals is the second priority in the audit process. These will control the scope of the efforts within the context of the classification of the audit. Focusing the goals to be around specific policies will ensure that the audit has a tangible work product. For example, if we are to evaluate the policy of unauthenticated queries can be run against our database we have a target that can be validated and verified. The work product for this step will be a list of testable statements that align to existing policies.

# Process

## Prepare

For each of the goals a set of tests are to be constructed that will validate that the policy as stated is being enforced. This will require a business process awareness and an adherence to the predefined scope of the audit.

## Audit

A non-exhaustive list of components of a database that will be part of the preparation evaluation. This should help identify various tiers of the database ecosystem to review. The auditors and management will need to evaluate this and identify mechanisms associated with these tiers for review.

* Server Maintenance
* Account Administration
* Access Control
* Data Privileges
* Passwords
* Encryption
* Activity

## Report

The target audience for this report will re-encapsulate the stated goals of the audit, the policies it aligns to, and the testing criteria. This report shall include all information within it so as to reduce drift due to external changes to policies, infrastructure changes, and other aspects. Audits are a point in time review at systems that change.