



**KAFOURY, ARMSTRONG & CO.**  
A PROFESSIONAL CORPORATION  
CERTIFIED PUBLIC ACCOUNTANTS  
8329 WEST SUNSET ROAD, SUITE 210  
LAS VEGAS, NEVADA 89113  
702.384.7717 FAX: 702.384.7718  
www.kafoury.com

Board of Trustees  
Southern Nevada Health District  
Las Vegas, Nevada

In planning and performing our audit procedures related to the basic financial statements of the Southern Nevada Health District (the "District"), we considered the District's system of internal controls in order to determine our audit procedures for the eventual purpose of expressing our opinion on the basic financial statements and not to provide assurance on internal controls.

During our audit, we noted two matters involving internal controls and other operational matters that are presented for your consideration. This recommendation is provided solely as information to assist the District in its pursuit for continuous improvements of internal controls and other operating procedures. This letter does not affect our report dated November 5, 2008 on the basic financial statements of the Southern Nevada Health District.

We have already discussed these comments with various District personnel, and we will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations. Responses to our recommendation have been provided by District staff and are included below for your convenience. We will review the status of the District responses during our next audit engagement.

## **CURRENT YEAR RECOMMENDATION**

### **Capital asset reconciliation**

#### **Observation**

The District maintains a capital asset inventory listing and computes the related depreciation by using a capital asset and depreciation software. The listing is reviewed on an annual basis to the physical assets. Annually, usually at fiscal yearend, a report is generated showing the capital asset, the current year depreciation provision and the fiscal year ending accumulated depreciation. This

report is support for financial statement prepared documents. Presently, the reports being generated excludes the beginning capital asset cost and related accumulated depreciation balance which then does not allow for an adequate reconciliation between the software beginning balances and the prior year audited financial statements ending balances.

### **Recommendation**

Management should reconcile the beginning capital asset and accumulated depreciation balances from the software generated report to the prior fiscal year end audited financial statements.

### **District's Response**

Staff is in the process of updating the software system to ensure that prior year balances are reconciled with the audited financial statements. Staff will continue to reconciling the balances at least annually.

### **Information Security Policies and Procedures**

#### **Observations**

We noted that standardized written procedures and policies were not available. In some cases appropriate procedures are indicated as being followed; however, the procedures are informal and not documented. The District understands the importance and are taking steps towards a more complete set of policies and procedures.

A small department with limited resources may actually be effective only because of the reliability of a key person. In the absence of well-defined procedures and key persons, the District may be vulnerable to system malfunctions, loss of data integrity, and security violations, such as loss of personal information confidentiality. Written procedures help to ensure that appropriate maintenance and corrective measures are routine and standards are established.

#### **Recommendations**

We suggest the District implement, an information security program to produce a set of standard policies and procedures. These should include, but not to an exclusion of other relevant areas, the following items:

- Limits for IT personnel to initiate or authorize transactions.
- Change control and incident management.
- Programmer access to production data.

- Password policies.
- Human resource management of persons having sensitive privilege responsibilities.
- Specific methods and means of transmitting and storing sensitive information electronically, such as through the use of encryption.
- Security monitoring practices, such as through the use of intrusion detection or prevention tools.
- System and data recovery. To ensure that information processing can be recovered and resumed after operations have been interrupted, emergency, backup and recovery plans should be documented and tested on a regular basis. These activities help ensure they remain current and operational.

#### **District Response**

The Health District is committed to implementing standard of Policies and Procedures for Information Security and is currently updating the written documentation. All items will be reviewed to ensure that the District is not vulnerable to any systems malfunctions and/or security violations.

In addition to this, the Health District is implementing an updated Password and Workstation security polices starting December 1st. Under the Password policy all Health District staff will be required to change their passwords on a quarterly basis. The Workstation security policy provides instructions on how to protect sensitive data on their workstations. These updated policies will assist with the security of the district's data and network integrity.

*Kofoony, Armstrong & Co.*

Las Vegas, Nevada  
November 5, 2008