## 1.0 General Information

### 1.1 Executive Summary

FOX3T has an Electronic Document Retention Policy in regards to the company's proprietary documents and records. These measures were put in place to ensure that all records and documents related to FOX3T are first off properly maintained and secured. Secondly, records that are no longer needed must be discarded at the designated time. The policy also aides' employees and for them to understand the rules and the roles they play in the process. Employees need to understand the restrictions and that the document types include: web files, text files, PDF documents, multimedia files, and Microsoft Office files.

### 1.2 Duration of Internal Audit

The duration of this internal audit will be for 10/14/16 commencing on 12/16/16.
It is anticipated that the fieldwork, working papers and drafting of deliverables will be completed by Oakmont  Audit Associates.

## 2.0 Internal Audit Objective and Scope

### 2.1 Internal Audit Objective

The purpose of the audit was to determine whether FOX3T has properly created and abided by what was written in their Electronic Retention Plan. The goal was to implement appropriate management practices and assist in providing designated controls to ensure disposing of data in a timely and secure manner.

### 2.2 Internal Audit Scope and Approach

On Nov 22, 2016, the IT Governance Committee and CISO of Fox3T will sign off on agreement to allow Oakmont LLP to audit Fox3T Electronic Retention policy, which will specifically include the following areas and associated parties

A. Accounting Finance
B. Corporate Records
C. Project Documentation
D. Source Code and Designs
E. Correspondence and Internal Memoranda
F. Legal Files and Papers
G. Data Destructions
H. Retention of Encrypted Data

## 2.3 Audit Plan for Fox3T

| Audit Matrix | | |
|---|---|---|
| **Control Area and Goal** | **Implemented Control** | **Testing Frequency** |
| **Accounting and Finance:**<br>These documents are maintained for a period of 7 years, 2 years or permanently, as per "The Massachusetts Society of Certified Public Accountants, Inc. Federal Taxation Committee | A document management system (Relativity) is implemented so documents are centrally saved and located on these servers. The data from the servers are being remote journaling to the backup site in New Mexico. A full backup is done weekly and incremental is done during the week. The last week of the month a monthly backup is done. These tapes are shipped to Iron Mountain for storage. All data that is at rest, in motion, or in storage is using 128 AES encryption. Audits are performed yearly by the Security group to verify the integrity and availability of the documents.<br><br>*Note: As per as per "The Massachusetts Society of Certified Public Accountants, Inc. Federal Taxation Committee. We decide to use their guild line for Accounting and Finance, Corporate Records, Project Documentation, and Legal Files and Papers. | Annually |
| **Corporate Records:**<br>These documents are retained for a period of 7 years after expiration or termination, current version only, or permanently, as per "The Massachusetts Society of Certified Public Accountants, Inc. Federal Taxation Committee | | |
| **Project Documentation (Microsoft Office Suite, PDF files and non-text/formatted files):**<br>Project Documentation is very important to the success of the project at Fox3T, so the retention period is 6 years. Other files like text/formatted files should be retained for 5 years. | | |
| **Legal Files and Papers:**<br>These documents are maintained for a period of 10 years, 10 years after the close of matter, 10 years after expiration of appeals or permanently, as per "The Massachusetts Society of Certified Public Accountants, Inc. Federal Taxation Committee | | |
| **Source Code and Designs:**<br>This information is pivotal to the Fox3T business so the goal is to permanently retain this information. | Source Code and Designs have the same controls implemented like the other documents except it has 256 AES encryption. Audits are completed quarterly by the Security group to verify the integrity and availability of the documents. | Quarterly |
| **Correspondence and Internal Memoranda (Electronic Mail/IM Messages and Web Page Files):**<br>These documents should be retained for the same period as the document they pertain to or support. Those pertaining to routine matters and having no significant lasting consequences should be discarded in two years, but documents that pertain to non-routine matters or having significant lasting consequences should generally be retained permanently. Electronic Mail/IM messages are retained for 90 days and Web Page Files are deleted every two weeks. | Correspondence and Internal Memoranda have the same controls implemented as per the other documents. Electronic Mail uses a 128 AES encryption; as well as, Digital Guardian, which is the DLP solution used to track data at rest, in transit and in storage. A script via PowerShell is ran every two weeks on all the machines deleting the browser history.<br><br>*Note: These documents are classified in a way that Digital Guardian has rules setup to send alerts to the Security group distribution list. The PowerShell script also sends a report of the machines that it couldn't contact to the Security group distribution list. | Quarterly |
| **Data Destructions:**<br>Exercising due diligence and due care when destroying data that has been retired or no longer of value. | We have partnered with Iron Mountain to dispose of any electronic or physical documents. Once Iron Mountain has destroyed the information they send us a certificate stating the destructions of the data. | Monthly |

* Note: All of these should be included in testing.

## 2.4 Audit Plan Execution

| General Computer Controls | | | |
|---|---|---|---|
| **General Control Area** | **Test of Controls** | **Control Evaluation** | **Notes on Results** |
| **Accounting and Finance**<br>**Corporate Records**<br>**Project Documentation (Microsoft Office Suite, PDF files and non-text/formatted files)**<br>**Legal Files and Papers** | The audit team will need to see the reports of the users who have access to the records. We will audit the backup plan by testing the restoration of data from the current backup, along with the procedures on how the backup is done during the month. We will also request the documentation that states the backups have been picked up on its current schedule by Iron Mountain. Verify that the encryption keys for the backups are valid and properly in a secure location. Request the document of the last audit report verifying the integrity, availability of the data and procedures on how verify the integrity of data. | Effective with conditions | The controls in place seem to be affected but there is limited documentation of procedures on how any of the controls are completed.<br><br>*Note: We will verifying this document exists. |
| **Source Code and Designs** | Verify the encryption keys can decrypt the data. List of users who have access to the keys and procedures on how the encryption process is done. Have the Security group reproduce the audit reports for the last year. | | |
| **Correspondence and Internal Memoranda (Electronic Mail/IM Messages and Web Page Files)** | Verify the encryption keys can reproduce to decrypt the data. List of users who have access to the keys and procedures on how the encryption process is done. Verify the logs in Digital Guardian tracking the classification of the data that is leaving the network via email. Verify that the PowerShell script removes the web pages' files from a random pool of machines. Produce the list of permissions of the users who access the PowerShell script. Check the rules in Digital Guardian to make sure they are classifying the documents properly and the reports that the PowerShell script produced in the last 6 months. | Effective | Need to include procedures in the policy |
| **Data Destructions** | Verify that Fox3T has and retained the certificates from Iron Mountain for the last year. | Effective with conditions | Where is the documentation stored and is it encrypted? |

* Note: All of these should be tested in current period.

## 2.5 Audit Plan Recommendations

There are two recommendations that the Oakmont group is suggesting for Fox3T Inc.,

1. Procedures should be clearly present and defined in the policy, especially for the controls that are in place to protect your data. In our assessment of the policy you have implemented the controls, but there is no documentation of procedures on how to use the controls.

2. Define roles and responsibilities of the security group in your policy. For instance, who created the PowerShell script to run on each machine to clear the web page files? Is this also the same person who verifies that the machine was connected to the network and the job was completed successfully? Another example who implemented and mages the DLP solution? If there is an issue, what is the chain of command within the security group? By identify a proper chain of command will help reduce confusion and improve efficiency when dealing with incidents or just getting general information.