ELECTRONIC DOCUMENT RETENTION POLICY

OCTOBER 18, 2016

FOX3T

I. Purpose

The purpose of this Policy is to ensure that necessary records and documents of the Fox3T, Inc. are adequately protected and maintained and to ensure that records that are no longer needed by Fox3T, Inc. or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of Fox3T in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

II. Scope

The scope of this policy covers all Fox3T, Inc. data stored on Fox3T–owned, Fox3T-leased, and otherwise company name provided systems media, regardless of location.

Note that the need to retain certain information can be mandated by local, industry, or federal regulations. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

III. Policy

This Policy represents the Fox3T, policy regarding the retention of records and the retention of electronic documents.

IV. Administration

Fox3T does not wish to simply adopt a "save everything" mentality. That is not practical nor cost effective, and would place an excessive burden on the IT Staff to manage the constantly-growing amount of data. The CISO and governance committee are in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Electronic Document Retention Policy is followed. The CISO is authorized to: make modifications to the Electronic Document Retention Policy from time to time to ensure that it is in compliance with local, state and federal laws and includes the appropriate document and record categories for Fox3T; monitor local, state and federal laws affecting record retention; annually review the record retention and disposal program; and monitor compliance with this Policy. As data storage increases in size and decreases in cost, companies often err on the side of storing data on local user's machine, on central file server, and again on backup systems. When identifying and classifying the Fox3T, it is important to also understand where the data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of information. Attached as Appendix A is a Record Retention Schedule that is approved as the initial maintenance, retention schedule for physical records of Fox3T and the retention schedule of electronic documents.

APPENDIX A – RECORD RETENTION SCHEDULE

The Record Retention Schedule is organized as follows:

Section Topic

A. Accounting and Finance
B. Corporate Records
C. Project Documentation
D. Source Code and Designs
E. Correspondence and Internal Memoranda
F. Legal Files and Papers

A. ACCOUNTING AND FINANCE

Record Type	Retention Period
Accounts Payable Ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Annual Audit Reports and Financial statements and General ledgers	Permanent
Annual Audit Records, including work papers and other documents that relate to audit	7 years after completion of audit
Annual Plans and Budgets	2 years
Bank statements, Canceled Checks and Employee Expense Reports	7 years
Interim Financial Statements and Notes Receivable ledgers and schedules	7 years
Investment records	7 years after sale of investment

B. CORPORATE RECORDS

Record Type	Retention Period
Corporate Records (minute books, signed Minutes of the Board and all committees, Corporate seals, articles of incorporation, bylaws, annual corporate reports, licenses and Permits, memorandums of understanding and annual reports)	Permanent
Contracts and Related Correspondence (including any proposal that resulted in the contract and all other supportive documentation	7 years after expiration or termination
Policy and Procedures Manuals – Original	Current version with revision history
Policy and Procedures Manuals – Copies	Retain current version only

C. PROJECT DOCUMENTATION

1. **Project Documentation:** including Microsoft Office Suite, PDF files, and non-text/formatted files retention also depends on the subject matter.
   - The length of time that any Word, Excel, PDF, or any other non-text/formatted file that has been created for a project and/or work product will be retained is 6 years. If any document is deemed as vital to performance, it should be stored on the Fox3T server.
   - **Text/formatted files** – The information security group will conduct annual reviews of all text/formatted files. These files will be copy from the network to our backup site and third party vendor for storage after each annual review. After five years these files will be deleted unless it's retained as per the governance committee. This does not include source code or design plans, please refer to Section D (SOURCE CODE AND DESIGN PLANS).

D. SOURCE CODE AND DESIGN PLANS

Source Code and Design plans are pivotal to the Fox3T company; this is why we must treat this information with the highest importance. When employees or contractors are creating, modifying, or distributing this information we need to make sure that all information is encrypted during rest, transit, and storage. The information security group will do a quarterly review of all these documents to make sure that the proper controls are in place to protect this information. This information will be permanently retained as per the governance committee.

E. CORRESPONDENCE AND INTERNAL MEMORANDA

Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, instructions for a particular project would be retained until the project is completed. It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project. If the project contains source code or design plans, please see Section D. (SOURCE CODE AND DESIGN PLANS).

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These are divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded within two years.
2. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.

Please note that copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed, unless that information provides reference to or direction to other documents and must be kept for project traceability.

Electronic Mail/IM messages: Not all email needs to be retained, depending on the subject matter.

- Employees are encouraged to manage their mail so they are keeping only business related information.
- Employees are prohibited from storing e-mail, IM messages or any corporate document that is deemed confidential on non-work related computers unless approved by the Fox3T.
- Employees are prohibited from sending confidential/proprietary Fox3T information to outside sources.
- Non-work related e-mail/IM messages will be retained for a maximum of 90 days. After 60 days the data will be moved to our backup site and a copy to our Third Party vendor storage company. After 15 days, the data will be deleted from the backup site. Then after another 15 days the copy will be deleted from our Third Party vendor storage company, as per the SLA.

Web Page Files: Internet Cookies

- All workstations: Internet Explorer, Chrome, or Mozilla should be scheduled to delete Internet cookies every two weeks.

F. LEGAL FILES AND PAPERS

Record Type	Retention Period
Legal Memoranda and Opinions (including all subject matter files)	10 years after close of matter
Litigation Files	10 years after expiration of appeals or time for filling appeals
Court Orders	Permanent
Requests for Department from Records Retention Plan	10 years

V. Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that Fox3T will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be. Exactly how certain data should be destroyed is covered in the Data Classification Policy and the Fox3T Record Management Policy.

When the retention time frame expires, the Fox3T must actively destroy the data covered by this policy. If an employee feels that certain data should not be destroyed, they should identify the data to their manager so that an exception to the policy can be reviewed. Since the decision has long term legal implications, exceptions will be approved only by a member or members of the company name executive team.

The Fox3T prohibits users not to destroy data in violation of this policy. Particularly forbidden is the destruction of data that a user may feel is harmful to themselves or destroying data in an attempt to cover up a violation of law, legal hold or company policy.

VI. Retention of Encrypted Data

The information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained. All data uses 128 bit AES encryption.

VII. Applicability

This policy is part of the company name cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed. This policy applies to electronic records generated in the course of the Fox3T operation, including both original documents and reproductions. It also applies to the physical records.

VIII. Enforcement

This policy will be enforced by the CISO and/or Fox3T Committees. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, Fox3T may report such activities to the applicable authorities.

IX. Revision/Review History

Revision	Date
Revision 1.0	10/4/2016
Revision 1.2	10/15/2016
Revision 1.3	10/17/2016
Revision 1.4	10/18/2016