SENSITIVE AND NON PUBLIC INFORMATION POLICY

1. PURPOSE

The company adopts this policy to help protect employees, customers, contractors and the company from damages related to loss or misuse of sensitive information. This policy will:

- Define sensitive information
- Describe the physical security of data when it is printed on paper
- Describe the electronic security of data when stored and distributed

2. SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at the company, including all personnel affiliated with third parties.

3. POLICY

3.1. Definition of Sensitive Information

Sensitive Information includes the following items whether stored in electronic or printed format:

3.1.1 Personal Information – Sensitive information consists of personal information including, but not limited to:

3.1.1.1. Credit Card Information, including any of the following:

- Credit Card Number (in part or whole)
- Credit Card Expiration Date
- Cardholder Name
- Cardholder Address

3.1.1.2 Tax Identification Numbers, including:

- Social Security Number
- Social Insurance Number
- Business Identification Number
- Employer Identification Numbers

3.1.1.3 Payroll Information, including, among other information:

- Paychecks
- Pay stubs
- Pay rates

3.1.1.4 Cafeteria Plan Check Request and associated paperwork

3.1.1.5 Medical Information for any Employees or Customers, including but not limited to:

- Doctor names and claims
- Insurance claims
- Prescriptions

- Any related personal medical information

3.1.1.6 Other Personal Information belonging to Customers, Employees and Contractors, examples of which include:

- Date of Birth
- Address
- Phone Numbers
- Maiden Name
- Names
- Customer Number

3.1.2 Corporate Information – Sensitive corporate information includes, but is not limited to:

3.1.2.1 Company, employee, customer, vendor, supplier confidential, proprietary information or trade secrets.

3.1.2.2 Proprietary and/or confidential information, among other things includes: business methods, customer utilization information, retention information, sales information, marketing and other Company strategy, computer codes, screens, forms, information about, or received from, Company's current, former and prospective customers, sales associates or suppliers or any other non-public information. Proprietary and/or confidential information also includes the name and identity of any customer or vendor and the specifics of any relationship between and among them and the company.

3.1.3 Any document marked "Confidential," "Sensitive", "Proprietary", or any document similarly labeled.

3.1.4 The company personnel are encouraged to use common sense judgment in securing the company confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor/manager.

3.2 Hard Copy Distribution

Every employee and contractor performing work for the company will comply with the following policies:

3.2.1 File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.

3.2.2 Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday.

3.2.3 Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.

3.2.4 Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.

3.2.5 When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD) approved shredding device. Locked shred bins are labeled "Confidential paper shredding and recycling". If you need any assistance in locating one of these bins, please contact a supervisor/manager.

3.3. Electronic Distribution

Every employee and contractor performing work for the company will comply with the following policies:

3.3.1 Internally, sensitive information may be transmitted using approved company email. All sensitive information must be encrypted when stored in an electronic format.

3.3.2 Any sensitive information sent external must be encrypted and password protected and only to approved recipients. Additionally, a statement such at this should be included in the email, "*This message may contain confidential and/or proprietary information, and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."*

4. ROLES AND RESPONSIBILITIES

Management will have the responsibility to enforce this policy and ensure that is is followed by employees and contractors.

5. DEFINITIONS

Encryption The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain test.

Hard Copy A printout of data stored in a computer. It is considered *hard* because it exists physically on paper, whereas a *soft* copy exists only electronically.

6. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Use of Confidential Information by Employee

As an employee of East Texas Baptist University, do hereby acknowledge that I must comply with a number of State and Federal Laws which regulate the handling of confidential and personal information regarding both customers/clients of this company and its other employees. These laws may include but not limited to FACTA, HIPAA, The Economic Espionage Act, The Privacy Act, Gramm/Leach/Bliley, ID Theft Laws (where applicable), Trade Secrets Protections, and Implied Contract Breach.

I understand that I must maintain the confidentiality of ALL documents, credit card information, and personal information of any type and that such information may only be used for the intended business purpose. Any other use of said information is strictly prohibited and is cause for immediate dismissal. Additionally, should I misuse or breach, any personal information of said clients and/or employees; I understand I will be held fully accountable both civilly and criminally, which may include, but not limited to, Federal and State fines, criminal terms, real or implied financial damages incurred by the client, employee, or this company.

I further agree to follow the rules and regulations this company has in place as regards to the handling of confidential information so as to protect the privacy of all involved.

_____	_____
Name	Witness
_____	_____
Signature	Date