EDS Data Security

Policies and Procedures

Version 2

Provided by:
ImageTrend, Inc.
20855 Kensington Blvd.
Lakeville, MN 55044
Tel: (952) 469-1589
Toll Free: (888) 469-7789
Fax: (952) 985-5671
www.imagetrend.com

TABLE OF CONTENTS

Table of Contents 2

Data Security Policy Overview 3

Application Security 5

- Data Warehouse Security 5
- Field Collection Security 7

Hosting Overview 8

Server Monitoring 9

Server Incident Response 10

Audit Functionality 11

System Backups 12

Disaster Recovery 15

Testing Processes 16

- Software Security Vulnerability Testing 16
- ADA Testing Process 16

Information Sensitivity Policy 17

Physical Security of Office and Hosting Site 22

Remote Access Policy 23

Roles and Responsibilities 25

Incident Report Mechanism 26

Support Services 28

ImageTrend Hosting Diagram 31

Copyright 33

DATA SECURITY POLICY OVERVIEW

This document defines the data security policy of ImageTrend, Inc. ImageTrend, Inc. takes the privacy of our employees and clients very seriously. To ensure that we are protecting our corporate and client data from security breaches, this policy must be followed and will be enforced to the fullest extent.

Intent

The goal of this policy is to inform ImageTrend employees and customers of the rules and procedures relating to data security compliance.

The ImageTrend data covered by this policy includes, but is not limited to all electronic information found in e-mail, databases, applications and other media; paper information, such as hard copies of electronic data, employee files, internal memos, and so on.

The Client data covered by this policy includes, but is not limited to all electronic information collected by any ImageTrend software application, which is hosted at the ImageTrend data center.

Audience

This policy applies to all employees, management, contractors, vendors, business partners and any other parties who have access to company and/or client data.

Data Types

ImageTrend, Inc. deals with two main kinds of data:

1. **Company-owned data** that relates to such areas as corporate financials, employment records, payroll, etc.
2. **Private data** that is the property of our clients and/or employees, such as social security numbers, credit card information, contact information, patient data, etc.

Data Classifications

ImageTrend, Inc.'s data is comprised of 3 classifications of information:

1. **Public/Unclassified.** This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, annual reports, corporate financials, and other data as applicable.

   Employees may send or communicate a public/unclassified piece of data with anyone inside or outside of the company.

2. **Private.** This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organizational charts, company policies, and other data as applicable.

   All information not otherwise classified will be assumed to be Private.

   Employees may not disclose private data to anyone who is not a current employee of the company.

3. **Confidential.** This is defined as personal or corporate information that may be considered potentially damaging if released and is only accessible to specific groups [e.g. payroll, HR, etc]. Confidential data includes, but is not limited to, social security numbers, contact information, tax forms, accounting data, security procedures [and other data as

applicable]. ImageTrend, Inc. considers it a top priority to protect the privacy of our clients and employees

Employees may only share confidential data within the department or named distribution list and with proper authorization.

4. **Secret/Restricted.** This is defined as sensitive data which, if leaked, would be harmful to ImageTrend, Inc., its employees, contractors, and clients. Access is limited to authorized personnel and third parties as required. Secret/restricted data includes but is not limited to audit reports, legal documentation, business strategy details, patient data, and other data as applicable.

   Secret/restricted data cannot be disclosed by anyone other than the original author, owner or distributor.

It is the responsibility of everyone who works at ImageTrend, Inc. to protect our own and client data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

Responsibilities

All employees are responsible for adhering to the policy and reporting any activities that do not comply with this policy.

Management is responsible for ensuring that their direct reports understand the scope and implications of this policy. HR must also ensure that all employees attend data privacy training and have evidence thereof and a signed copy of this policy in their file.

Security staff will be monitoring data for any unauthorized activity and are responsible for updating access requirements as needed.

Any employee who authors or generates corporate or client data must classify that data according to the criteria outlined above.

Management

Ownership of this policy falls to Security Officer. For any questions about this policy, or to report misuse of corporate or personal data, please contact him/her at (952) 469-1589. The IT department will work in conjunction with the client to maintain data access privileges, which will be updated as required when an employee joins or leaves the company. These are the accepted technologies ImageTrend, Inc. used to enforce and ensure data security:

1. Access controls
2. Strong passwords
3. System monitoring
4. Personnel Training

Review

Management is responsible for keeping this policy current. This policy will be reviewed annually or as circumstances arise.

On an annual basis, unless previous action was required, we review our security policies and procedures to ensure that necessary updates have occurred. We welcome any security reviews that our customers might request at their expense. Several clients have performed such reviews over the years and have been satisfied with the results.

Enforcement

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

APPLICATION SECURITY

DATA WAREHOUSE SECURITY

EMS State Bridge/EMS Service Bridge/Rescue Bridge
The ImageTrend applications meet or exceed State and federal data privacy requirements and the HIPAA guidelines. Secure logins are an industry standard process and are part of the HIPAA guidelines for data protection. These are implemented throughout the application with the use of the multi-tiered hierarchical security access features of the ImageTrend security module, which provides the environment for controlling the access necessary to provide data protection.

The reporting and auditing functions of the application's procedures allow for safeguarding and immediate notifications of any attempted breaches. This provides for data access only through assigned permissions and ensures that only those intended see their data and can access it for reporting.

Application Securities

- Secure User Login
- Password Encryption
- Password Requirements
- Login Expirations
- Page Access Checking
- SSL Server Certificate: 128-bit encryption Security Certificate
- CAD data sent using secure Web Service

Permissions Administration

Manage Users and Groups
The application employs a hierarchical based password administration as a series of group policies to control application entry and level of access within the application. With the system administrator being the highest level of security, groups can be created below that to encompass all other group needs, which may include:

- Director – Access to view all runs within their service.
- Multiple Service Administrators – User Access and administration to multiple services.

Permissions and Rights
Permission and rights are governed by the ability of what the user can see and do. At the global level, rights are based on the following criteria:

- County
- City
- Service

On the service level, there are two levels:

- Administrator
- User

Service administrators can control and edit all the functions with their own service. Service users have the ability to edit and view their own information.

Password Administration
Through the Application Access Control, the system administrator can determine several features regarding the password administration:

- Number of days without login to the application before the user's account is suspended
- Number of attempts a user can attempt to login before their account is placed on temporary suspend
- Set the password to contain at least one numeric character
- Set the pass word to contain at least one uppercase character
- Number of past passwords stored in the log table for a user
- Number of passwords in the log table to be compared with the newest password to prevent repeat use of passwords
- Minimum number of characters in the password
- Number of days the user will be notified before they must change their password
- An Email Confidentiality statement can be added, edited and deleted
- An inactive account message can be added, edited and deleted
- Security questions prompt on login or password retrieval
- Encrypt security question answer

Procedural Securities

Hosting Environment

ImageTrend's Web applications are hosted in our state-of-the-art 4,500 square foot data center. Built in a vault with 21" concrete walls, our facilities offer the maximum level of security and stability for hosting needs. The data center features triple redundant, high-speed internet connections over fiber optic trunk lines. Only authorized personnel have access to the data floor. The data center is monitored electronically, as well as a log book is kept to monitor and record individuals accessing the server room.

ImageTrend's production network consists of application/web and database servers. The databases are on a private network with access control managed through the firewall permitting only authorized administrators or approved VPN access.

Applications are monitored for availability and performance from multiple locations to ensure an accurate measure of current system health. Slow application pages and long running database queries are logged for analysis by server administrators and development staff. Serious errors and performance degradation trigger email alerts which are sent to support staff and cell phone alerts to ImageTrend's 24/7 X-Team Support staff. Our X-Team support employees have VPN access to our production servers, to ensure accessibility and security, when accessing our servers from outside of our network.

Auditing

The system’s audit trail tracks user information when accessing the secure portion of the application. IP address, User ID, date/time, browser information, along with information on each file accessed, is all tracked within a separate database, which is kept for a period of time for reporting purpose and audit trails.

Any security breaches are logged within our Project Management system for any HIPAA disclosures related to security breaches or information disclosers. If a security breach happens, the security module currently sends an email to our Director of Development and the Security Officer, who in turn notifies the designated customer contact.

FIELD COLLECTION SECURITY

EMS Field Bridge
Security for Field Bridge conforms to the current best practices and new technology. Security enhancements have been performed both behind the scenes with increased database security and through settings that administrators can configure for automatic run removal and password requirements.

Data Storage Security
Data storage for each Field Bridge works with Microsoft SQL CE 2008. This software provides greater data security for all patient data. The databases contained within SQL CE 2008 are password protected to prevent unauthorized access and the entire database is completely encrypted with 128-bit encryption. In addition, all patient data within the database is further encrypted using Rijndael (AES) cipher algorithm using a 128-bit key and IV, assemblies are obfuscated and string encrypted. Data received through a CAD integration is sent via secure Web Services.

Data Sync to Service/Rescue/State Bridge
The ImageTrend EMS Field Bridge complies with W3C web Service and XML standards. Data is synced from the Field Bridge to the Service/Rescue/State Bridge through secure web service communication utilizing 128-bit SSL Certificate which encrypts all data during transmission.

There are three authentication parameters that are required to be sent with the web service request as outlined below. A user account will be set up within the Field Bridge system to track access and assign any actions to a particular user. An additional API token will be created for web service authentication.

- token=uniqueidentifier
- userID=string
- password=string

Administrative-Set Security Options
Administrators have the ability to configure the Field Bridge to provide additional security. Additional security is possible based on your service's IT departments and policies.

Clearing Out Old Incidents
Administrators can choose to delete old incidents from the Field Bridge database after a certain number of days and after those incident reports have been posted to the Service Bridge, State Bridge or Rescue Bridge system working with this Field Bridge. Automatically removing old incidents will reduce the amount of patient data available in the system at any one time without causing any additional time to manually clean out the database, reducing any risk of a security issue.

Usernames and Passwords
Within the Field Bridge, any user who wants to work with the application must log in with a username and password set up on the Service Bridge, State Bridge or Rescue Bridge to which this Field Bridge is assigned. Administrators can set up the password requirements, the length of time in between required password changes and any restrictions on the user's access to portions of the Field Bridge.

HOSTING OVERVIEW

ImageTrend's hosting environment provides 99.9% availability and is comprised of state-of-the-art Blade Servers and SAN storage that ensure this with software and infrastructure virtualizations, blade computing redundancies and backup storage policies. Our data center service is recognized by Microsoft as being in the top 100 of their “Top Tiered Hosting Partners”.

Our Compellent SAN has a fiber channel backend, currently hosts 8TB of storage, has dual storage controllers with redundant power supplies and redundant paths to disk, and hot swappable drives. We do offsite replication to disk on a second SAN. Information will be stored in the system for as long as desired by the client. Archived information will still be accessible by the System Administrators. Data will only be purged upon a client request.

Hardware
ImageTrend server hardware is configured to prevent data loss due to hardware failure and utilize the following to ensure a quick recovery from any hardware related problems.

- Independent Application and Database Servers
    - Microsoft SQL Server 2012
    - Microsoft Windows Server 2008
- Redundant Power Supplies
- Off-Site Idle Emergency Backup Servers (optional)
- Sonicwall VPN Firewall
- Redundant Disk configuration
- Weekly, monthly or quarterly backups (as contracted)
- Periodic CD-ROM backups (as contracted)
    - Weekly, monthly or quarterly
    - Offsite vaulting and escrow
- 30 GB Disk Space allocation per month with additional space in 10 GB increments
- 3 Mb Traffic or Bandwidth per month with additional bandwidth available in 1 Mb increments

Physical Facility
ImageTrend's Web applications are hosted in our state-of-the-art 4,500 square foot data center. Built in a vault with 21" concrete walls, our facilities offer the maximum level of security and stability for hosting needs. The data center features triple redundant, high-speed internet connections over fiber optic trunk lines. Only authorized personnel have access to the data floor. The data center is monitored electronically, as well as a log book is kept to monitor and record individuals accessing the server room.

- Redundant, high-speed Internet connections over fiber optics.
- Power protection via an in-line 80kVa UPS with a 150 KW backup diesel generator
- Temperature controlled
- Waterless Fire Protection and Clean agent fire suppression
- Secured site access
- Steel Vault Doors
- 21" concrete walls and ceiling

Data Integrity
ImageTrend applications are backed up daily allowing for complete recovery of data to the most recent backup:

- Daily Scheduled Database and Application Backups.
- Daily Scheduled backup Success/Failure notification via cell-phone and email

SERVER MONITORING

This section outlines the process followed to ensure server stability and proactively reduce server incidents.

Server Status
All ImageTrend production servers are monitored 24/7 for system health and service availability. Status information includes:

- current users accessing the system
- disk use
- memory use
- CPU use
- Notification of hardware failures

Server logs are kept on a separate server and are available for review even in the event that a server fails for forensic use in determining the state shortly before a problem occurred. Server status is recorded and any dramatic change in a metric generates an alert message to all available support staff.

Application Status
All ImageTrend production servers are monitored 24/7 for the status of Web services and ImageTrend applications. Status information includes:

- application availability
- application response time
- failure status codes

A change in application status generates an alert message to all available support staff. General application responsiveness is tested, not individual client sites are monitored, so an error in a single application may go undetected by this system.

Monitoring Intervals and Response Times
Monitoring events occur between every three and eight minutes depending on the application and server being monitored. Monitoring takes place from multiple locations with staggered start times resulting in a monitoring resolution of approximately two to five minutes. Alerts generated by the monitoring system are sent to support staff via email and SMS to cell phones, with an average transmission time of one minute.

SERVER INCIDENT RESPONSE

Service Recycling
The most common cause of service unavailability is a failed service. A failed service is given 10 minutes to recycle or the problem is escalated to a server restart. Other action may be taken as the situation warrants, given service specific errors or an obvious cause for the failure.

Server Restart
A server restart should be undertaken if a service recycling does not solve the failure or further troubleshooting. Normal operating system functions for restarting should be used if possible. Otherwise using ImageTrend’s remote controllable power outlets the server should be cold booted. The progress of the restart is observed using ImageTrend’s IP enable KVM switch allowing BIOS or other hardware errors to be observed and worked through.

Transferring Websites
If within 50 minutes of the initial alert being issued services have not been restored and a solution does not appear to be immediately forthcoming, the services and roles of the unavailable server will be moved to an alternate location. ImageTrend maintains an extra server capacity to allow for this flexibility with minimal disruption to other services. If the original files are unavailable backups will be used to recreate the original server configuration. As the same IP addresses are used to restore service no DNS changes are required and the restoration is immediate. While in transition the websites affected will display a message describing the problem and an estimation of the time to service being restored.

Transferring Locations
If service cannot be restored by transferring to a different server within the same environment, services will be moved to an alternate hosting location. A backup datacenter is available in Chicago, IL, for hosting mission critical applications. Code and database backups are pushed to this location to be used in the event of disaster which disables the primary datacenter in Minneapolis, MN. Clients requiring automatic failover can opt for DNS failover which detects service unavailability and automatically moves DNS records to refer to the backup location. Other clients will be moved to the backup datacenter as needed and DNS changes will be made manually or requested immediately upon the initiation of relocation.

Hardware Replacement
Whenever a hardware failure contributes to a server failure the hardware in question will be replaced aggressively before redeploying the system. For instance, a failed drive will be replaced; multiple drive failure will require all drives be replaced as well the power supply and possibly drive cables if damage is evident. If a system operates for an extended period without cooling fans the system components will be retired from production use and completely replaced.

AUDIT FUNCTIONALITY

Our site monitor audit trail tracks user information when accessing the secure portion of the application. IP address, User ID, date/time, browser information, along with information on each file accessed, is all tracked within a separate database, which is kept for a period of time for reporting purposes and audit trails.

Any security breaches are logged within our Project Management system for any HIPAA disclosures related to security breaches or information disclosures. If a security breach happens, the security module currently sends an email to our Director of Development and the Security Officer, who in turn notifies the designated customer contact.

There are also numerous reports for data import to track user, date/time, import type, number of records, validity, and total import time.

Audit Reports Available

- Audit Report
- Validity Audit Report
- Field Audit Report
- Run Report
- Run Variance Report

When run incidents enter the system, they are tracked on both date and time and the user that entered that run. It will also track the date/time that a user that last updated that information. In addition to the audit trail, there are addendum and attachment features within the system. Addendums allow staff to enter additional text to track changes within an existing run report, or attach any necessary files.

A history trail for each run report tracks staff usage including date/time and user for:

- Generating PDF Run Reports
- Adding addendums
- Changing run status
- Changing run lock status
- Adding attachments
- Viewing repeat patient

SYSTEM BACKUPS

ImageTrend provide backup coverage for continuity purposes as well as data archive purposes. Define backup and retention policies to clearly establish expectations of coverage. Define continuity resources and locations. Meet or exceed contract and other obligations.

Code Backups

Application code is backed up daily; at least a daily backup exists for all applications hosted in ImageTrend's production environment and is included in hosting costs. These backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. Daily backups are retained for longer as unallocated storage permits but not guaranteed to be available beyond the previous calendar day. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Database Backups

Database files are backed up daily; at least a daily backup exists for any database hosted in ImageTrend's production environment and is included in hosting costs. Daily backups are retained for several days as unallocated storage permits but not guaranteed to be available beyond three previous calendar days. Database backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Restore Procedures

Daily backup files are stored uncompressed to facilitate quick recovery of one or more files as needed. Archive copies are compressed to conserve disk space. All database files are compressed to conserve disk space and must be uncompressed and reattached for restoration. When restoring a file the newer file, if it exists, is renamed and kept before replacing with the backup version. When restoring an entire database file, the copy being replaced is itself backup up before being modified. When restoring part of a database file, the current file is first backed up and the backup database is mounted with a different name, then the needed tables are restored and the backup file is detached. If restoring a complete backup of application code over a corrupted install, a copy of the bad files is kept to maintain any new user-added files since the backup was created.

Backup Goals

ImageTrend has several goals for our backup coverage:

- Provide simple and rapid continuity resources
- Provide adequate backup coverage to meet contract and other obligations
- Substitute redundant active resources for continuity backups where reasonable
- Clearly define specific backup policies which differ from the standards
- Maintain a backup window with minimal impact on performance and availability

Minimal Backup Contents

Backups for all data must include:

- One copy of current application files, updated nightly and stored on separate disks from those hosting the application

- One copy of current database files, updated nightly and stored on separate disks from those hosting the database
- One copy of current system configurations, updated nightly and stored on separate disks from those hosting the system
- Alternate retention policies for a specific application must be laid out in writing, specifying requirements for frequency of backups, retention period and coverage requirements

Archive Backup by category

Standard

- No archive required (0)
- Week of daily archives recommended (8)
- Archives- Minimum: 0, Recommended: 8

Important

- Two weeks of daily archives required (15)
- One month of weekly archives required (4)
- Six months of monthly archives required (6)
- Two months of weekly and 1 year of monthly archives recommended (8,12)
- Archives- Minimum: 25, Recommended: 34

Critical

- Four weeks of daily archives required (29)
- Three months of weekly archives required (12)
- 1 year of monthly archives required (12)
- 1 year of weekly archives recommended (52)
- Archives- Minimum: 53, Recommended: 76

Optional

- No continuity or archives required
- Single continuity backup recommended
- Archives- Minimum: 0, Recommended: 1

Continuity Backup by category

Standard

- Continuity restoration within hours

Important

- Continuity restoration within one hour

Critical

- Continuity restoration within 30 minutes

Optional

- No continuity or archives required

Offsite backup by category

All offsite backups are stored encrypted on disk in a locked fire cabinet in ImageTrend's offices or replicated to other collocation sites per the following categories.

Standard

- Monthly offsite backup is stored

Important

- Monthly offsite backup is stored, offsite replication may be performed per availability requirements

Critical

- Monthly offsite backup is stored, offsite replication may be performed per availability requirements

Optional

- Optical disc based or electronic transmission backups sent to clients may be performed on a negotiated schedule

Terms	**Definitions**
Continuity Backup	An exact and current as possible copy of all files, data and system configurations comprising an application
Data Archive Backup	Stored backups for the purposes of restoring data to a specific point in the past
Full Backup	A complete copy of all data at that moment in time
Incremental Backup	A copy of all new or modified files since last full or incremental backup
Differential Backup	A copy of all new or modified files since last full backup
Week of daily archives	previous week’s full backup, this week’s full backup and the past six day’s nightly differential backups
Weekly archive	Full backup made on single day of the week (e.g., Sunday morning)
Monthly archive	Full backup made on single day of the month (i.e. the First of the month, or first Sunday of the month)

DISASTER RECOVERY

ImageTrend, Inc. follows a specific critical path for organizations and companies during a recovery effort, to ensure the resumption of normal operations in the event of a disaster. This process has seven stages, which are followed regardless of the organization.

ImageTrend' EMS solutions consist of EMS State Bridge and Field Bridge, hosted at our facilities. In a disaster recovery plan it is important to minimize the loss of data and return application usage as quickly as possible.

Stage 1 - Immediate Response
The first step in the recovery process and the initial reaction to a potential disaster or interruption consists of immediate assessment and if necessary, notification of clients of interruption and any actions they should undertake. In many situations the system's redundancies will accommodate the situation and provide continuity. This takes place within the first 4 hours.

Stage 2 - Environment Restoration
The necessary steps for restoring service via repairs or alternate infrastructure are begun by gathering the necessary components for restoration and installing. If local repair is not possible due to extreme conditions, then the service will be redirected to another data center and the required DNS redirection may take up to 8 hours to propagate.

Stage 3 - Functional Restoration
Application functionality is tested on restored or alternate service site to ensure user access and usability. For same data center restoration within 8 hours and for alternate site usage within 24 hours.

Stage 4 - Data Restoration and Synchronization
This step includes backlog reduction. Data from offsite locations is restored to the restored environment. Database backups are automatically done every 2 hours, daily and weekly. These backups will be used for data restoration and synchronization. Maximum data window will be two hours. Most often, data is protected at different times during the business cycle and must be reconstructed or synchronized before it can be used. Synchronizing, validating, and reviewing data from many different sources is a critical step in a successful recovery. Once reliable data is established, backlogged transactions that have accumulated during recovery can be processed. This may take up to 48 hours, however application usage is available during this time.

Stage 5 - Business Resumption
Clients will be notified that the affected service can now resume its normal operations.

Stage 6 - Interim Site Migration
Once the primary site environment has been restored, return migration is planned and scheduled. Depending on the nature of the problem, this may take an extended period of time to restore the environment. Disruption of services during this transition will be minimized and clients will be notified of the impact and a schedule of return will be mutually discussed.

Stage 7 - Return to Home Site
All recovery efforts have been completed, and a business may resume normal operations at its primary location.

TESTING PROCESSES

SOFTWARE SECURITY VULNERABILITY TESTING

ImageTrend understands the importance of data security and consistently addresses the latest advances in regulations and technologies to ensure that our systems and processes meet federal and state data security standards. Our application security is designed to OWASP best practices and our hosting infrastructure is the latest 3-tier firewall configuration. Application access utilizes 128 bit encrypted secure socket layers and data transfers are encrypted as well. Our QA includes the use of IBM AppScan, which provides:

- Static analysis security testing to identify vulnerabilities at the source
- Automated web application scanning and testing with intelligent fix recommendations
- Extended coverage through Glassbox analysis and JavaScript Security Analyzer
- Automated correlation of static and dynamic analysis results

Security reviews have been conducted by several individual government organizations prior to their purchase of our applications with satisfactory results.

ADA TESTING PROCESS

ImageTrend follows ADA WCAG 2.0 level conformance guidelines. Resources are created and designed using xml, css, mathml, SMIL, SVG and other open standards that have features to support accessibility by people with disabilities. The client-facing pages follow the standards set in the ADA WCAG 2.0 accessibility guidelines to level AA conformance. ImageTrend performs audits of its product’s accessibility and works to improve its conformance through regularly scheduled product upgrades. As with all of its products, ImageTrend, Inc. extends an ongoing effort to conform application to Level AA – ADA Conformance for Web Content Guidelines. We offer all of our clients the opportunity to perform testing on our web based applications to determine compliance with their own policies, needs, and/or requests. Should these tests result in modification or enhancement requests, they will be reviewed as to applicability within our planned product roadmap or handled as client-specific requests.

INFORMATION SENSITIVITY POLICY

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of ImageTrend without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, information on paper and information shared orally or visually (such as telephone and video conferencing).

All employees familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect ImageTrend Confidential information (e.g., ImageTrend Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager.

Data Privacy

ImageTrend respects and understands the need for data privacy and the methods and functions needed to ensure this for both ImageTrend data and Client data. Software application, data center infrastructure, policies and procedures all play an integral role in this. Our staff reviews all updates whether from our partners (Microsoft and Adobe), federal and state legal opinions and guidelines or standards organizations to ensure that we are continually informed of the latest requirements. Our designers and developers continually monitor best practices and technological advances to ensure data privacy. ImageTrend's data center is located in a bank vault and has all of the physical controls in place to ensure security. Our staff is trained in the needs and processes required for data privacy and are all subjected to background checks.

On an annual basis, unless previous action was required, we review our security policies and procedures to ensure that necessary updates have occurred. We welcome any security reviews that our customers might request at their expense. Several clients have performed such reviews over the years and have been satisfied with the results.

HIPAA Training

All ImageTrend employees are subjected to background checks and are required to attend and successfully complete HIPAA training. The ImageTrend Project Management System gives us a facility to track any HIPAA Security Incidents or Information Disclosure Incidents for reporting purposes.

Only those certified ImageTrend employees that work with either hardware or software related to the specified application or project will access the data center and interact with our servers. These employees have worked with our hardware as part of our IT support staff or are part of our Implementation team as software developers. Authorization is granted from the management level.

Scope

All ImageTrend information is categorized into two main classifications:

- ImageTrend Public
- ImageTrend Confidential

ImageTrend Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to ImageTrend Systems, Inc.

ImageTrend Confidential contains all other information. Confidential information is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Information that should be protected very closely includes trade secrets, development programs, potential acquisition targets and other information integral to the success of our company. Also included in ImageTrend Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of ImageTrend Confidential information is "ImageTrend Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to ImageTrend by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders and supplier information. Information in this category ranges from extremely sensitive to information about connecting a supplier/vendor into ImageTrend's network to support our operations.

ImageTrend personnel are encouraged to use common sense judgment in securing ImageTrend Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should contact their manager.

Policy

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as ImageTrend Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the ImageTrend Confidential information in question.

Minimal Sensitivity

Minimal sensitivity data includes general corporate information and some personnel and technical information.

Marking guidelines for information in hardcopy or electronic form

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential."

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "ImageTrend Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "ImageTrend Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, ImageTrend information is presumed to be "ImageTrend Confidential" unless expressly determined to be ImageTrend Public information by an ImageTrend employee with authority to do so.

Guidelines for Minimal Security Data

- **Access**. Granted to ImageTrend employees, contractors, people with a business need to know.
- **Distribution within ImageTrend**. Allowed in standard interoffice mail, approved electronic mail and electronic file transmission methods.
- **Distribution outside of ImageTrend internal mail**. Allowed with U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

- **Electronic distribution.** No restrictions except that it is sent to only approved recipients.
- **Storage**. Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
- **Disposal/Destruction**. Deposit outdated paper information in specially marked disposal bins on ImageTrend premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure.** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

More Sensitive
More sensitive data includes business, financial, technical and most personnel information

Marking guidelines for information in hardcopy or electronic form
Note: any of these markings may be used with the additional annotation of "3rd Party Confidential."

As the sensitivity level of the information increases, in addition to or instead of marking the information "ImageTrend Confidential" or "ImageTrend Proprietary," you may wish to label the information "ImageTrend Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Guidelines for More Sensitive Data

- **Access.** Granted to ImageTrend employees and non-employees with signed non-disclosure agreements who have a business need to know.
- **Distribution within ImageTrend.** Allowed with standard interoffice mail, approved electronic mail and electronic file transmission methods.
- **Distribution outside of ImageTrend internal mail.** Can be sent via U.S. mail or approved private carriers.
- **Electronic distribution.** No restrictions on sending to approved recipients within ImageTrend, but should be encrypted or sent via a private link to approved recipients outside of ImageTrend premises.
- **Storage.** Individual access controls are highly recommended for electronic information.
- **Disposal/Destruction.** Allowed in specially marked disposal bins on ImageTrend premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure.** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code and technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form
Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

To indicate that ImageTrend Confidential information is very sensitive, you may should label the information "ImageTrend Internal: Registered and Restricted", "ImageTrend Eyes Only," "ImageTrend Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of ImageTrend Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Guidelines for Most Sensitive Data

- **Access.** Granted to only those individuals (ImageTrend employees and non-employees) designated with approved access and signed non-disclosure agreements.
- **Distribution within ImageTrend.** Must be delivered direct — signature required, envelopes stamped confidential or approved electronic file transmission methods.
- **Distribution outside of ImageTrend internal mail.** Must be delivered direct; signature required; approved private carriers.
- **Electronic distribution.** No restriction to approved recipients within ImageTrend, but it is highly recommended that all information be strongly encrypted.
- **Storage.** Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
- **Disposal/Destruction.** This is strongly encouraged: Should be in specially marked disposal bins on ImageTrend premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure.** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Terms	Definitions
Appropriate measures	To minimize risk to ImageTrend from an outside business connection, ImageTrend computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access ImageTrend corporate information, the amount of information at risk is minimized.
Configuration of ImageTrend-to-other business connections	Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.
Delivered Direct; Signature Required	Do not leave in interoffice mail slot; instead, call the mail room for special pick-up of mail.
Approved Electronic File Transmission Methods	Includes supported FTP clients and Web browsers.
Envelopes Stamped Confidential	You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.
Approved Electronic Mail	Includes all mail systems supported by the IT Support Team. If you have a business need to use other mailers contact the appropriate support organization.
Approved Encrypted email and files	Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within ImageTrend is done via a license. Please contact the appropriate support organization if you require a license.
Company Information System Resources	Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information

and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac, you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of ImageTrend.

Encryption

Secure ImageTrend Sensitive Information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a onetime password token to connect to ImageTrend's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that ImageTrend has control over for its entire distance. For example, all ImageTrend networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. ISDN lines to employees' homes are private links. ImageTrend also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies with which ImageTrend has established private links include all announced acquisitions and some short-term temporary links

PHYSICAL SECURITY OF OFFICE AND HOSTING SITE

Entrances

Facility and office entrances are kept to a minimum to control access. ImageTrend's main entrance is planned with access control systems and procedures in mind. Reception desk and other controls help to maintain security at ImageTrend's front entrance. The other entrances at the ImageTrend office are only accessible by employees with keys.

Access Controls

At every perimeter entrance, locking devices and controls are in place to ensure security is sustained. Key control is an essential part to ImageTrend's access control. Only ImageTrend employees are given a key that cannot be replicated. Before 8:00 am and after 5:00pm all ImageTrend entrances are locked. To get in or out before 8:00 am or after 5:00pm employees need to unlock the door to enter, and then relock the entrance behind them.

Exterior Security

ImageTrend equips the building with security cameras that run 24/7. These security cameras monitor activities outside the building to provide views of approaching pedestrian and vehicular traffic, building entrances, and departing pedestrian and vehicular traffic.

Physical Security of Hosting Site

All visitors of Implex.net are greeted and asked to sign in with photo ID. The visitors are escorted around the facility by an Implex.net employee. The Implex.net site has video surveillance and two controlled doors with key card access.

All visitor information, not just the sensitive information, is restricted to Implex.net developers, network operations personnel and other qualified employees (such as billing clerks or customer care representatives). Finally, the servers on which Implex.net stores personally identifiable information are kept in a secure location.

The DataSafe is Implex.net's main data center where they collocate servers and host client web sites on their shared servers. The entry to the Implex.net DataSafe was built inside a bank vault and is thoroughly encased by 21" reinforced concrete walls. The vault doors are fully functional.

REMOTE ACCESS POLICY

The purpose of this policy is to define standards for connecting to ImageTrend's network from any host. These standards are designed to minimize the potential exposure of ImageTrend to damages that may result from unauthorized use of ImageTrend resources. Damages include the loss of sensitive or company confidential data, loss of intellectual property, damage to public image, damage to critical ImageTrend internal systems, etc.

Scope

This policy applies to all ImageTrend employees, contractors, vendors and agents with an ImageTrend-owned or personally-owned computer or workstation used to connect to the ImageTrend network. This policy applies to remote access connections used to do work on behalf of ImageTrend, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH and cable modems, etc.

Policy

General

It is the responsibility of ImageTrend employees, contractors, vendors and agents with remote access privileges to ImageTrend's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to ImageTrend.

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods and of acceptable use of ImageTrend's network:

- Acceptable Encryption Policy
- Virtual Private Network (VPN) Policy
- Wireless Communications Policy
- Acceptable Use Policy

For additional information regarding ImageTrend's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

Requirements

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases whenever possible. Use of a username/password combination is acceptable for access when DACL’s are applied. For information on creating a strong passphrase see the Password Policy.

- At no time should any ImageTrend employee provide their login or email password to anyone, not even family members.
- ImageTrend employees and contractors with remote access privileges must ensure that their ImageTrend-owned or personal computer or workstation, which is remotely connected to ImageTrend's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- ImageTrend employees and contractors with remote access privileges to ImageTrend's corporate network must not use non-ImageTrend email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct ImageTrend business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the ImageTrend network must meet minimum authentication requirements of CHAP.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
- All hosts that are connected to ImageTrend internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
- Personal equipment that is used to connect to ImageTrend's networks must meet the requirements of ImageTrend-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the ImageTrend production network must obtain prior approval from Remote Access Services and InfoSec.

Term **Definition**

Cable Modem Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP Challenge Handshake Authentication Protocol (CHAP) is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel.

Dial-in Modem A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing Having concurrent connectivity to more than one network from a computer or network device. Examples include: being logged into the Corporate network via a local Ethernet connection and dialing into AOL or other Internet service provider (ISP); being on an ImageTrend-provided Remote Access home network and connecting to another network (such as a spouse's remote access); or configuring an ISDN router to dial into ImageTrend and an ISP, depending on packet destination.

DSL Digital Subscriber Line (DSL) is another form of high-speed Internet access. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay A method of communication that can go incrementally from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN There are two flavors of Integrated Services Digital Network (ISDN): BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access Any access to ImageTrend's corporate network through a non-ImageTrend controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-ImageTrend network (such as the Internet or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into ImageTrend's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

ROLES AND RESPONSIBILITIES

Roles of system administrators in terms of their responsibility for defining and securing access for users are as follows:

Role	Responsibilities
Administrators (X-Team)	Full access to infrastructure, operating systems and supporting applications
Implementation	Full control of code, database tables and supporting applications
Level 1 Support	User level access to the ImageTrend application
Level 2 Support	Admin level access to the ImageTrend application and limited access to the supporting applications
Level 3 Support	SuperAdmin rights to the ImageTrend application read rights to the database and can change accounts and permissions

INCIDENT REPORT MECHANISM

Effective response and collective action are required to counteract security violations and activities that lead to security breaches. ImageTrend shall provide timely and appropriate notice to affected clients when there is reasonable belief that a breach in the security of private information has occurred. A breach in security is defined as an unauthorized acquisition of information, typically maintained in an electronic format by ImageTrend.

Purpose
The ultimate goal of security incident response and centralized reporting is to protect data and prevent obstruction of government operations. It is important to distinguish between problems that stem from mistakes or miscommunications and true security incidents that involve either malicious intent or intent to circumvent security measures

Scope
Attacks on ImageTrend resources are infractions of the Acceptable Use Policy constituting misuse, or they may be vandalism or other criminal behavior. Reporting information security breaches occurring on ImageTrend systems and/or on ImageTrend networks to appropriate authorities is a requirement of all persons affiliated with ImageTrend in any capacity, including staff, students, faculty, contractors, visitors, and alumni.

General
Suspected or confirmed information security breaches must be reported to ImageTrend. ImageTrend will investigate the report, and if a security breach of private and/or highly sensitive information may have occurred, will inform the IT Manager and/or law enforcement, as appropriate.
In the event that a public notification of the security breach may be warranted, the IT Manager will consult with the appropriate ImageTrend employees to develop the response and make the final determination if a public notification of the event is warranted.

Procedures
The entity responsible for support of the system or network under attack is expected to:

- Report the attack to their management and to the IT Manager
- Block or prevent escalation of the attack, if possible
- Follow instructions communicated from the IT Manager in subsequent investigation of the incident and preservation of evidence
- Implement recommendations from the IT Manager
- Repair the resultant damage to the system

Internal Notifications
ImageTrend's employees will report serious computer security breaches to the IT Manager in a timely manner. The IT Manager will consult with one or more VP's as appropriate, and decides if the Management Team must be convened to determine a response strategy, or if an alternate group is appropriate for the response. This determination may be made prior to completion of the investigation of the security breach.

External Notification
Determination of External Notification
To determine if unencrypted private or highly sensitive information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, the (likelihood of the) following will be considered:

- Physical possession (lost or stolen device?)
- Credible evidence the information was copied/removed
- Length of time between intrusion and detection

- Purpose of the intrusion was acquisition of information
- Credible evidence the information was in a useable format
- Ability to reach the affected individuals
- Applicable University policy, and/or local, state, or federal laws

External Notification
If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

- Written notice will be provided to the affected individuals using US Mail, unless the cost is excessive or insufficient contact information exists. The letter will be developed by the department responsible for the system experiencing the breach, and approved by the Management Team and others as appropriate. The excessiveness of cost consideration will be the decision of the IT Manager, Management Team, and President for.

If written notice to the affected individuals is not feasible, the following methods will be considered for providing notice:

- Personal e-mail notices (provided addresses are available), developed by the department responsible for the system experiencing the breach, and approved by the IT Manager, Management Team, and other administrators as appropriate.
- A press release to media, to be written by Marketing and approved by the IT Manager, and other administrators as appropriate.
- An informational web site, developed and hosted by the department responsible for the system experiencing the breach, and approved by the IT Manager, Management Team, and others as appropriate, with a conspicuous link in the ImageTrend News area.
- All expenses associated with external notification will be the responsibility of the department responsible for the system that experienced the security breach.

SUPPORT SERVICES

ImageTrend provides both support for their applications and hosting as contracted. Support includes technical diagnosis and fixes of technology issues involving software and server hardware. ImageTrend has a broad range of technical support and proposes to provide service in the areas of:

- Website Hosting and Support
- Web Application Development/Enhancement
- Database Administration/Support
- Project Management
- Systems Engineering/Architecture

Product Support

ImageTrend will provide ongoing support as contracted after installation for the customer. This includes continued attention to product performance and general maintenance. ImageTrend offers multi-level technical support, based on level-two user support by accommodating both the general inquiries of the administrators and those of the system users. We will give the administrators the ability to field support for the system as the first level of contact while providing them the option to refer inquiries directly to ImageTrend.

ImageTrend's Support Team is available 24/7 at support@imagetrend.com and www.imagetrend.com/support as well as Monday through Friday from 7:00 am to 7:00 pm CST at:

Toll Free: 1-888-469-7789
Phone: 952-469-1589

Support Desk

ImageTrend offers an online support system, Support Desk, which incorporates around-the-clock incident reporting of all submitted tickets to ImageTrend's support desk specialists. Once a client submits a support ticket, he or she can easily track its progress with a secure login, promoting a support log for the client and ImageTrend's support team. The system promotes speedy resolution by offering keyword-based self-help services and articles in the knowledgebase, should clients wish to bypass traditional support services. Ticket tracking further enhances the efforts of Support Desk personnel by allowing them to identify patterns which can then be utilized for improvements in production, documentation, education and frequently asked questions to populate the knowledgebase. The support ticket tracking system ensures efficient workflow for the support desk specialists while keeping users informed of their incident's status. Support patterns can be referenced to populate additional knowledgebase articles.

Upgrades and New Version Releases

ImageTrend offers updates and new version releases to customers subscribing to our support agreements. On average, these updates occur once a quarter. These updates offer new product enhancements and improvements. Customers are notified in advance of these potential changes in order for them to be aware of any impact this may have on them and to schedule the upgrade. The Fire Bridge, if hosted at our facilities, is upgraded by our personnel; however clients are notified prior to the upgrade for scheduling purposes. If the Fire Bridge is hosted at your facilities, then we assist in the upgrade either through remote login or an onsite visit if required (incurs travel costs).

The contents of the updates are determined by customer request levels and necessity. The EDS Users Group, comprised of field EMT's and Paramedics, has also been instrumental in providing insight for determining the necessity and value of requested product enhancements.

ImageTrend support agreements include software updates, so that applications continually offer the latest technology and provide new features. We encourage all clients to take advantage of these updates. Products will be maintained for the client as long as they have a valid support agreement.

X-Team Support
In addition to our standard services, ImageTrend's X-Team is available for after-hour's emergency support. Our X-Team will receive notifications of issues submitted to our Online Support Desk. If an issue is deemed non-critical by the X-team they may elect to respond during normal business hours or charge for after hour's resolution.

Problem Escalation and Resolution
ImageTrend has support available for clients via telephone, Support Desk and/or electronic mail during ImageTrend's normal business hours (7:00 a.m. to 7:00 p.m. Central Standard Time, Monday through Friday, excluding holidays). The Project Manager will address operational issues on an ongoing basis. Senior Management will handle issues requiring further discussion and resolution.

Incident Reporting
Malfunctions. ImageTrend makes all efforts to correct malfunctions that are documented and reported by the Client. ImageTrend acknowledges receipt of a malfunction report from a Client and acknowledges the disposition and possible resolution thereof according to the Service Level Agreement. If the Malfunction reported prevents all useful work from being done, or disables major functions from being performed, we undertake immediate corrective action to remedy the reported issue. If the malfunction reported represents a non-mission critical issue, reasonable corrective action to remedy the malfunction within three business days will be taken. If the malfunction reported disables only non-essential functions, resulting in degraded operations, we undertake reasonable corrective action to remedy the reported malfunction within a reasonable time period.

Submission. All support requests received by either direct phone contacts, Support Desk and support@imagetrend.com are recorded by client, incident description and disposition into our support log.

Support Log
Information regarding outstanding problems, fixes, modifications and improvements will be available to the Client electronically and published on a regular basis to a Project Support Log which will be available for Client's access.

ImageTrend University
ImageTrend provides online education materials for their products as self-guided tutorials to all clients with support agreements. These online support and educational materials can be found at ImageTrend University via your ImageTrend application. ImageTrend recently started implementing ImageTrend University throughout its solutions to promote ongoing education and training of our solutions. When accessing ImageTrend University through the application, users can view educational videos, manuals, quick guides and workbooks to assist them in better understanding our software and support train-the-trainer sessions. These have been very useful as both refresher and initial education materials. A sample demonstration of ImageTrend University can be found at www.imagetrend.com/university.

System Documentation
ImageTrend provides the most up-to-date documentation, including administrator and user manuals and release notes for any upgrades. With a support agreement, this documentation, along with educational videos, PowerPoint presentations and other documents will be found at ImageTrend University, which can be accessed from the State Bridge application. Any provided documentation becomes the property of the client. ImageTrend will provide a full set of documentation at each location upon request. Documentation updates are available online at no cost.

System Maintenance
Change Request. When a client makes a change request, we apply that to other users and their needs to determine if it would be beneficial to others in the EMS community – from the local volunteer organization to the regional users to mid and large size cities and state governments. If the requested change would be beneficial to the product as a whole, it may be included in a version release. For client-specific requests, we seek further mutual understanding. Sometimes product understanding meets the intended outcome of the change request or a work around is found. If neither of these meets the needs of the

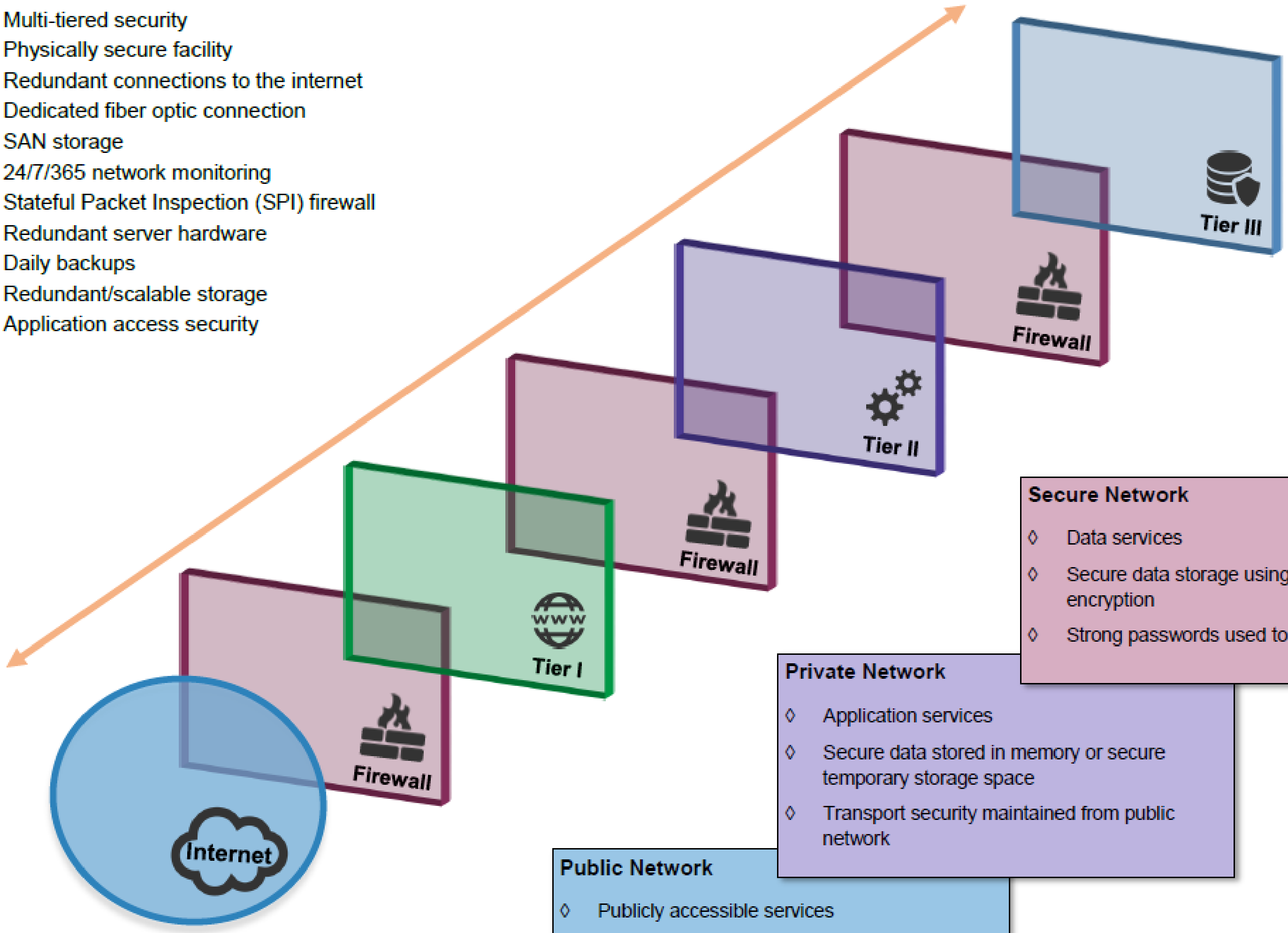
client, we can establish a Statement of Work to customize the application for the specific client for additional fees.

Support Staff. ImageTrend's support staff is made up of EMS and Fire professionals who are well versed in the technical aspects of our products. They are either well trained on the software, have used it in the field, or are the developers of the system.

IMAGETREND HOSTING DIAGRAM

Application Hosting Services

⇒ Multi-tiered security
⇒ Physically secure facility
⇒ Redundant connections to the internet
⇒ Dedicated fiber optic connection
⇒ SAN storage
⇒ 24/7/365 network monitoring
⇒ Stateful Packet Inspection (SPI) firewall
⇒ Redundant server hardware
⇒ Daily backups
⇒ Redundant/scalable storage
⇒ Application access security



Secure Network

◊ Data services
◊ Secure data storage using strong file encryption
◊ Strong passwords used to protect data

Private Network

◊ Application services
◊ Secure data stored in memory or secure temporary storage space
◊ Transport security maintained from public network

Public Network

◊ Publicly accessible services
◊ Minimal secure data stored, protected by file and transport encryption

IMAGETREND INC.

COPYRIGHT

ImageTrend Referenced Products

- EMS State Bridge
- EMS Service Bridge
- Rescue Bridge
- EMS Field Bridge

Viewer contains copyrighted materials, which are licensed to you, the end user, for your personal use subject to the terms of the enclosed end user license agreement. You must treat this software and its contents like any other copyrighted material, such as a Portfolio or musical recording. Any other use, duplication, or distribution of this product or its contents may violate applicable U.S. or international copyright laws, and may subject you to prosecution under penalty of law.

ImageTrend logos are a registered trademark, and is a trademark of ImageTrend, Inc.

NOTICE Unless otherwise provided by written agreement with ImageTrend, Inc., this publication, and the software sold with this publication, are provided "as is" without warranty of any kind either expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. The entire risk arising out of the user or performance of this publication and software remains with you. In no event will ImageTrend, Inc., or any of its suppliers, be liable for any lost profits, lost savings, direct, incidental or indirect damages or other economic or consequential damages, even if ImageTrend, Inc. or its suppliers have been advised of the possibility of such damages. ImageTrend, Inc. reserves the right to modify this document at any time without obligation to notify anyone.

IMAGETREND INC.