Evincesis Security Policy

Evincesis Security Infrastructure is broken down into the following Components

1. Confidentiality (Agent Level)
2. Monitoring Process (Agent and Infrastructure)
3. Audit and Control Process
4. Data Privacy (Customer)
5. Information Security Process and Standards

Confidentiality (Agent Level)

NDA – Client Level and Service Level
Information Access Control
Security Configuration Management
Security Management Process
Media Controls (no floppy drives or CD-Writers in any of the machines)
No Public Network (No Internet Access)

Monitoring Process (Agent and Infrastructure)

Defined Process
Documented processes for changing data once created and for the prevention of unauthorized manipulation of data, and audit trails should log unauthorized access and changes.
Documented storage processes and mechanisms; parameters defining when data should be destroyed or archived should be documented; and data disposal procedures, including hardware disposal, should be documented.
Local Call Barging
Remote Call Barging (Client Side)
Remote Screen Capture

Audit and Control Process

Audit Trail
Version Control
Extensive Logging Mechanism
Authorization (Login ID's and Password)
Authentication (Secure ID)

Data Privacy (Customer)

Centralized Data Storage
IP Level Security
Desktop Level Security controlled by a Domain
Authentication (Login ID's and Password)
Authorization
Logging (Can be enabled to monitor Keystrokes)
Additional AES 256 bit Encryption with PKI (if required) File and Database

Information Security Process and Standards

Chain-of-Trust Agreements
Contingency Planning
Records Processing
Information Access Control
Internal Audit
Personnel Security
Security Configuration Management
Security Incident Procedures
Security Management Process
Termination Procedures
Training (under several regulations)
Media Controls
Physical Access Controls
Access, Audit, Authorization, and Authentication Controls
Communications and Network Controls
Electronic/Digital Signature

Antivirus Strategy

NOD32 Corporate Edition
With roaming virus definition update capability
All nodes protected with Norton Antivirus with automatic Updates

All Vulnerable ports are blocked

Desktop Level Security

All nodes running on Windows 2000 Professional and Windows XP
Domain Login
User Privilege
Centralised Software Audit