

# Information Security & Management Systems

# Our Security Protocol

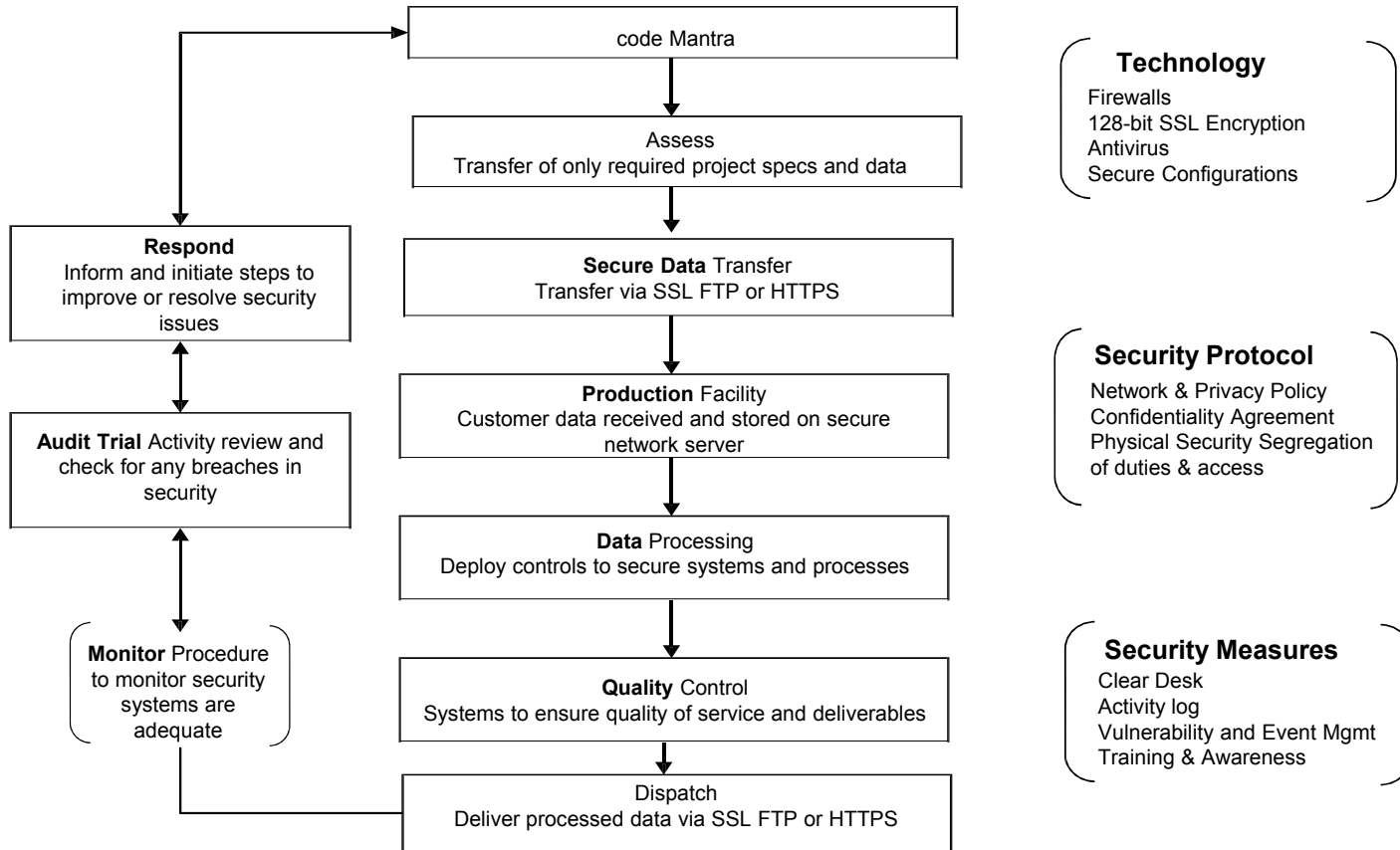
Network Security – Our entire network is protected by multiple-layer of security appliance and software.

We have implemented the following security technologies to ensure information security and confidentiality levels exceed compliance requirements.

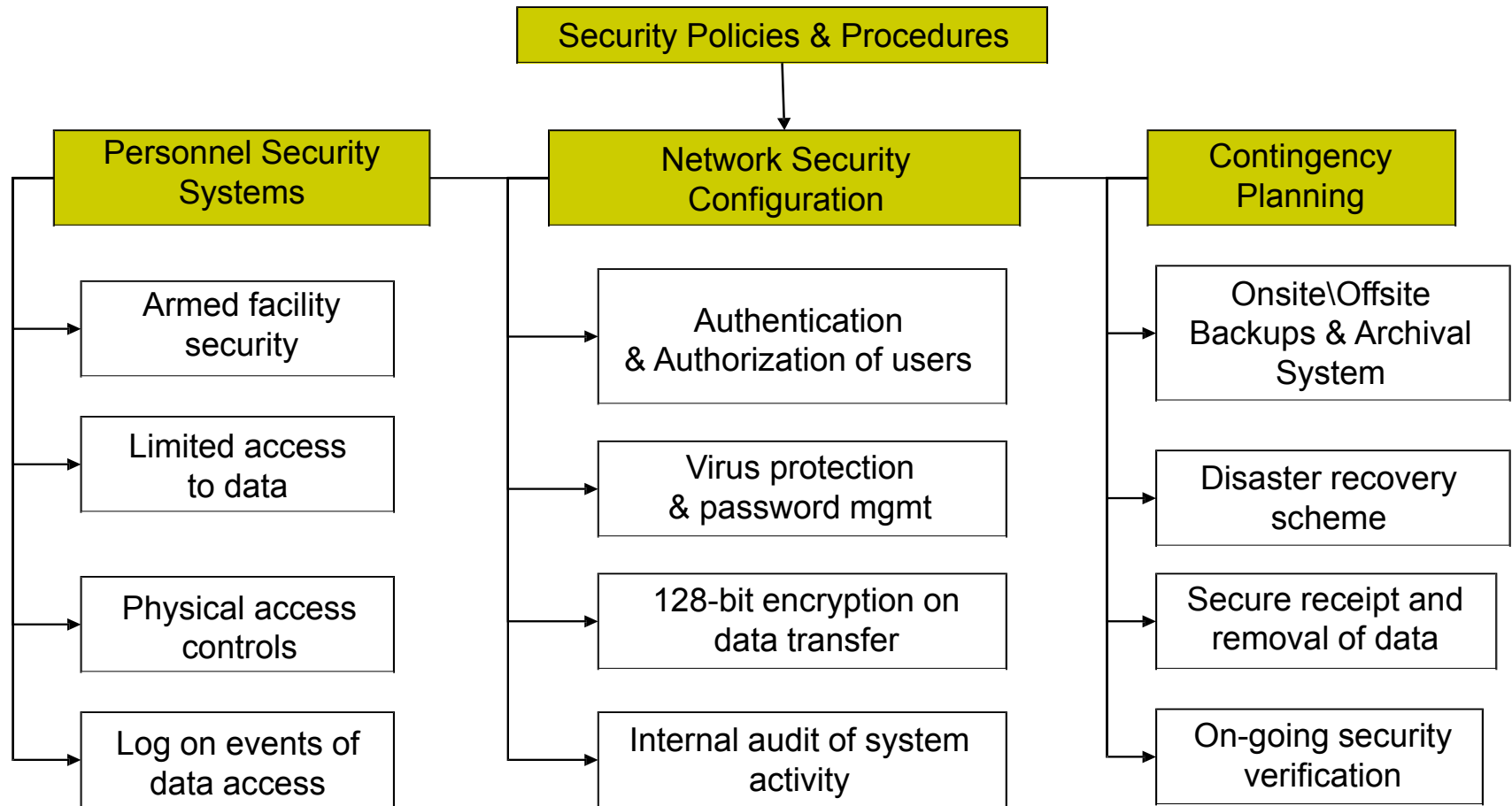
- Internet Security & Accelerator (ISA) Server.
- WatchGuard Firewall and Internet Security Appliance.
- Verisign's 128 –bit SSL encryption for online services.
- Cisco VPN with encryption for remote LAN-TO-LAN connections.



# Our IS Framework



# Network Policy Chart



# Network Resilience



Our high-end production servers are built with integrated RAID VI for data protection by supporting hard disk drive mirroring and redundant power models.

Data storage – As per our contingency plan, we run nightly backup on our servers.

Disaster recovery and back-up facilities to ensure business continuity.

Offsite backups - We have taken precautions disaster recovery measure to store critical data on secure offsite storage.

# Privacy Policy & Procedures

---

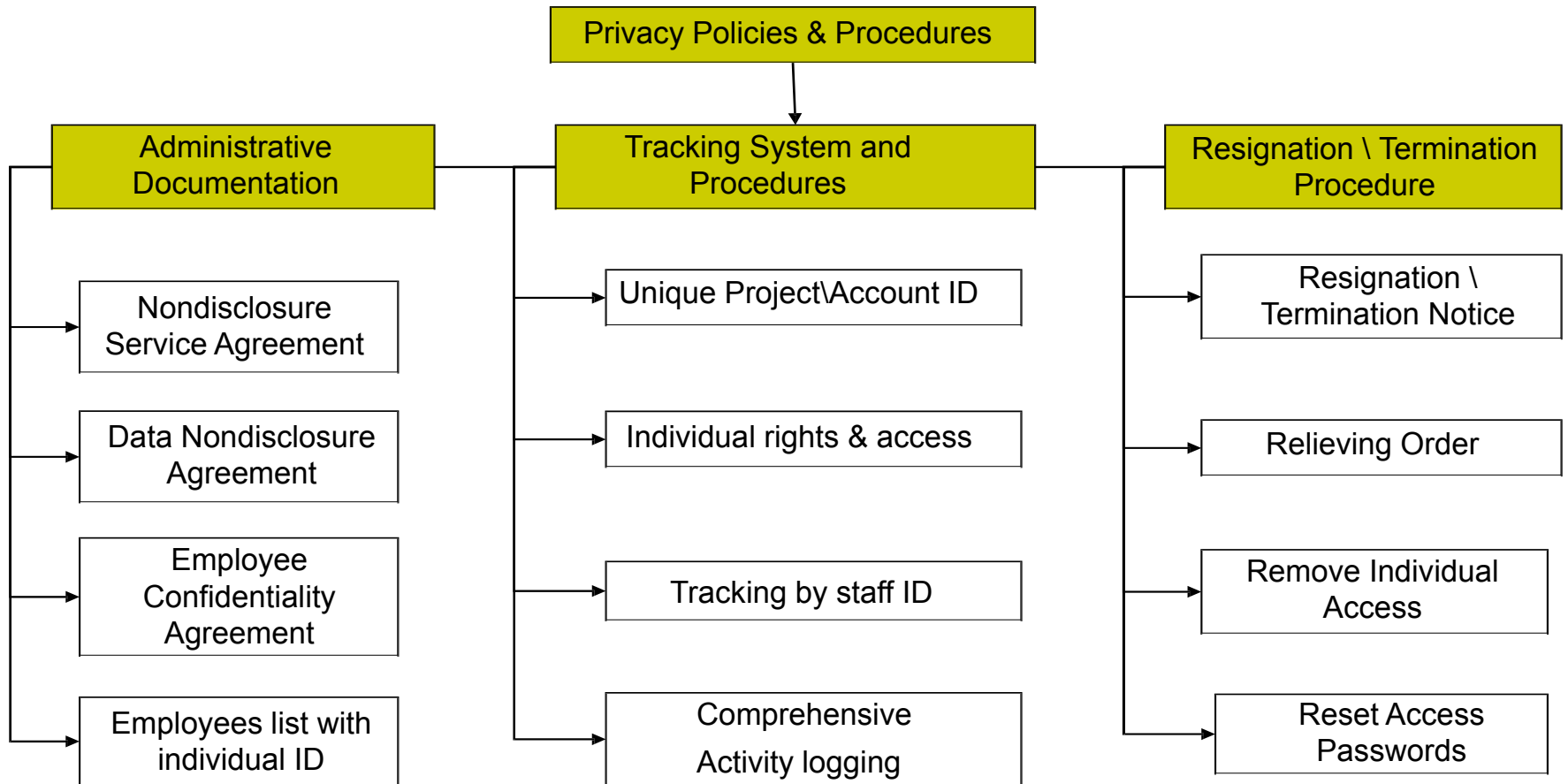


Our Privacy Policy includes,

A non-disclosure and confidentiality agreement to be signed by all members of the organization and senior management.

A data non-disclosure agreement to maintain the confidentiality of technical and business information.

# Privacy Policy Chart



# File Transfer Protocol



---

File Transfer Protocol – Our secure FTP server supports SSL File Transfer.

Secure Sockets Layer (SSL) security protocol enables encrypted data transfer using the FTP client applications like cuteFTP Pro, FTP Voyager, or WSFTP Pro.

This state-of-art SSL technology will encrypt the entire session using an implementation of SSL called Explicit Encryption (AUTH SSL). This protects confidential information from interception and hacking.

# Intruder Detection



---

Anti-virus System - we use leading products like Norton Anti-Virus and McAfee to protect the flow of information on PCs, file servers, web servers, FTP servers, and email servers.

We deploy periodic anti-virus\software update, real time scanning and monitoring to avoid any virus attach or intrusion resulting from new viruses.

Activity Monitoring – All the activity across the network is logged and reviewed regularly and any anomalies or discrepancies are thoroughly investigated.

# Office Security Systems



- ❑ All the entry points to the premises are guarded by armed security,24x7.
- ❑ Security cameras are installed at all critical points including production floors with digital recording capability.
- ❑ To ensure highest level of security and access to the premises, bio- metric finger-print access control system is installed at all entry and exit doors with anti-bypass facility.
- ❑ The building is installed with Fire Alarm \ Protection systems and emergency exits.
- ❑ NO Internet access at production nodes.
- ❑ NO floppy, NO Mass Storage devices, CD or media allowed inside production facility.
- ❑ Production computers are installed with strict local policy and unwanted storage of any client data is restricted.
- ❑ Emergency Medical Kit

# Business Redundancy



cM has a well planned and documented procedure outlining procedural and decision making regarding backup arrangements, resource allocation, priorities, and action items necessary to fulfill the goals of effective and timely disaster recovery, emergency management and business continuity plans.

Disaster Recovery and Business Redundancy Plans include:

- Daily backup of all new digital assets.
- Version control of process and deliverables at every stage.
- Backup of assets at secured off-site facility (Tapes, CDs/DVDs).
- Power backup with UPS and diesel powered generators.
- Hardware/Software support staff, 24 x 7.
- System maintenance procedures.
- 2 x 3Mbps Fractional E1, 2 x 512 kbps backup ADSL
- VoIP, secure FTP, SSL, & VPN capabilities

# Confidentiality & Privacy Compliance



- ❑ All our work is done with utmost confidentiality of data and stored in highly secure Information Servers and physical locations.
- ❑ Transmission of data through 128-bit encrypted SSL technology ensures high level of data security over Internet.
- ❑ We have non-disclosure and confidentiality agreements in place to ensure that client's data is revealed only to staff with proper expressed permission.

# Thank You



For more details, please contact

codeMantra, LLC  
600 West Germantown Pike  
Suite 400  
Plymouth Meeting, PA 19462-1046

Tel: 610-940-1700  
Fax: 215-243-6421  
E-mail: [cminfo@codemantra.com](mailto:cminfo@codemantra.com)  
Website: <http://www.codemantra.net>