# Data Security Standard

- Secure Network
  - firewall to protect cardholder data
  - we do not use default system password
- Protect Customer Data
  - All Customer Data stored in an high encrypted way (3DES,AES)
  - Deleting Customer data after not needed any more using Encrypted shredder
- Maintain Computer and Software
  - Use and regularly update anti-virus software on all systems
  - Updating Operating Systems
  - Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Restrict access to production and valuable material area
  - Each person assign with a unique ID and followed up with access tracking system
  - Restrict physical entrance access to production area
- Regularly Monitor and Test Networks
  - Track and monitor all access to network resources regularly
  - Regularly test security systems and processes
- Maintain Information Security
  - Maintain and update the security policy.