STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.01	Page 1 of 2
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Information Security Strategy	

Effective Date: October 9, 2012

Policy:
DEPARTMENT will implement safeguards determined to be reasonable and appropriate to protect its information assets to maintain the confidentiality, integrity, and availability (CIA) of those assets.

Security policies, plans, and procedures created in support of this Information Security Policy, are organized in five categories (sections) and address at a minimum:

- Administrative safeguards:
  - Security management process
  - Risk analysis
  - Risk management
  - Sanction policy
  - Information system activity review
  - Assigned security responsibility
  - Workforce security
  - Authorization and/or supervision
  - Workforce clearance procedure
  - Termination procedures
  - Information access management
  - Access authorization
  - Access establishment and modification
  - Security awareness and training
  - Security reminders
  - Protection from malicious software
  - Log-in monitoring
  - Password management
  - Security incident procedures
  - Response and reporting
  - Contingency plan
  - Data backup plan
  - Disaster recovery plan
  - Emergency mode operation plan
  - Testing and revision procedures
  - Applications and data criticality analysis
  - Evaluation
  - Business associate agreement and other arrangements
  - Written contract or other arrangement

- Physical safeguards
  - Facility access controls
  - Contingency operations
  - Facility security plan

    - Access control and validation procedures
    - Maintenance records
    - Workstation use
    - Workstation security
    - Disposal
    - Media re-use
    - Accountability
    - Data backup and storage

- Technical safeguards
    - Access control
    - Unique user identification
    - Emergency access procedure
    - Automatic logoff
    - Encryption and decryption
    - Audit controls
    - Integrity
    - Mechanism to authenticate sensitive information
    - Person or entity authentication
    - Transmission security
    - Integrity controls
    - Encryption

- Organizational Framework
    - Policies and Procedures requirement
    - Documentation requirement

- Data Breach
    - Data Breach Management
    - Data Breach Notification
    - Data Breach Notification to HHS
    - Data Breach Notification to Member
    - Data Breach Notification to Media

- Other Policies
    - Information classification
    - Network security
    - Email security
    - Wireless security

In addition, all security policies, and procedures shall be reviewed and evaluated (based on any environmental and operational changes) on an annual basis by the Information Security Officer and team.