

InfoSec Tutorial: Security Management

Tony Kenyon, CEO.

Revision 1.01.

Updated: Jan 5th 2006

Ref: CNXT0006

Security Management Practices

- **Roles**

- Systems & Information Owner
- Classifiers (owner, user etc)
- Issue/System specific policy

- Confidentiality levels

- Awareness->Training->Education

- Policies, Regs, Guidelines etc

- Security Life Cycle

- See OMB A-130 (3 year controls audit)

- See NIS 33 800-12,18,14,27,30

Security Management Practices

- **Management Concepts**
 - CIA: Confidentiality, Integrity & Availability
 - DAD: Disclosure, Alteration, Destruction
 - Identification, Authentication, Accountability, Authorization, Privacy
 - Security Controls

Security Management Practices

- **Information Classification: Government**
 - Unclassified
 - Sensitive but Unclassified (SBU)
 - Confidential
 - Secret
 - Top Secret
- **Information Classification: Private Sector**
 - Public Use
 - Sensitive
 - Private
 - Confidential

Security Management Practices

- Classification Criteria
 - Value, Age, Useful Life, Personal Association
- Distribution of Classified Info
 - Court Order, Government Contracts, Senior Executive Approval

Questions?