

Chapter 24

Information Technology Security Management

- | |
|--|
| ● Standards for categorizing information and information systems by mission impact |
| ● Standards for minimum security requirements for information and information systems |
| ● Guidance for selecting appropriate security controls for information systems |
| ● Guidance for assessing security controls in information systems and determining security control effectiveness |
| ● Guidance for certifying and accrediting information systems |

f24-01-9780123943972

Security Policy
Organization of Information Security
Asset Management
Human Resources Security
Physical and Environmental Security
Communication and Operations Management
Access Control
Information Systems Acquisition, Development and Maintenance
Information Security Incident Management
Business Continuity Management
Compliance

f24-02-9780123943972

Access Control Standards
Accountability
Audit Trails
Backups
Disposal of Media
Disposal of Printed Matter
Information Ownership
Managers Responsibility
Equipment
Communication
Procedures and Processes at Work

f24-03-9780123943972

Health Insurance Portability and Accountability Act (HIPAA)

Gramm-Leach-Bliley Act

Sarbanes-Oxley Act of 2002

Security Breach Notification Laws

Personal Information Protection and Electronic Document Act (PIPEDA)

Computer Fraud and Abuse Act

USA PATRIOT Act

f24-04-9780123943972

Maximum Penalty

Extent of Damage

Aggregation of Damage

Enhancement of Punishment

Damage to Foreign Computers

State Law Offenses

Expanding the Definition of Loss

Response

f24-05-9780123943972