



## Altius IT Policy Collection Compliance and Standards Matrix

Security Control	Altius IT Policy and Plan	ISO	NIST	Health	PCI
Governance	IT Governance Policy	§8.2 §A.6.1.2 §4.1 §5.1 §A.6.1.1	800-26 800-30 800-33 800-53A 800-60	164.308	12.4 12.5
Information Security	Privacy Policy Securing Information Systems Policy Security Controls Review Policy	§11.2.3 §A.10.8.1 §A.15.1.4	800-14 800-53A	422.112	12.1
Risk Management	Business Impact Analysis Risk Assessment Policy Risk Management Policy	§A.14.1.2 §4.2.1(c) §4.2.1(f)	800-14 800-53A	45 CFR §164.308 422.504 820.22	3.2 – 3.4 6.2
Policies and Procedures	Security Policy Security Policy Intro System Security Plan	§4.2.1 (b) §5.1 §A.5.1.1	800-14 800-34 800-53A 800-61	422.112 422.202	12.1- 12.4
Organization	IT Governance Policy IT Management Policy IT Support Staffing Policy	§4.2.2 (f) §A.6.1 §A.8.2.1 §A.8.1.1 §A.6.2	800-48 800-53A 800-88	422.503	12.4- 12.5
Asset Management	Data Classification Policy Network Access Policy Software Licensing Policy	§4.3.3 §7.2.1	800-14 800-18 800-26	21 CFR 11.1(b) 11.1(f)	3.3 3.4
Human Resources	Acceptable Use Policy Computer Training Policy IT Support Staffing Policy Social Networking Security Policy Third Party Service Providers Policy	§5.2.2 §A.6.1.1 §A.7.1.3 §A.8.2.2	800-14 800-26 800-53A	21 CFR §820.20b §820.75b §820.25a	12.6- 12.8
Physical and Environmental	Personnel Security Policy Physical Access Security Policy Physical Security Policy	§A.9.1.1 §9.1.4	800-14 800-53A	164.310	9.1- 9.10
Communications and Operations	Account Management Policy Anti-Malware Policy Backup Policy Data Integrity Policy Domain Controller Policy Domain Name System Policy E-commerce Policy Electronic Disposal Policy E-mail Policy Firewall Policy Internet Connection Policy Intrusion Detection Policy Logging Policy Mass Communication Policy Network Configuration Policy Network Documentation Policy Removable Media Policy Router Security Policy Security Monitoring Policy Server Hardening Policy Vendor Access Policy Workstation Security Policy	§9.1 §10.4.1 §10.4.1 §10.4.1 §10.7.2 §10.10.2 §10.7.4 §11.4.7	800-14 800-53 800-124	820-60 820-65	1.1- 1.4 2.1- 2.4 3.1 5.1- 5.2 8.1- 8.5 10.1- 10.7



## Altius IT Policy Collection Compliance and Standards Matrix

Security Control	Altius IT Policy and Plan	ISO	NIST	Health	PCI
Access Control	Admin Special Access Policy Asset Control Policy Identification and Authentication Logical Access Controls Policy Network Access Policy Password Usage Policy Portable Computing Policy Remote Access Policy Securing Information Systems Policy Securing Sensitive Information Policy Smartphone & Mobile Device Policy System Update Policy User Privilege Policy Web Policy Wireless Access Policy	§11.3.1 §11.5.3 §11.4.5 §11.4.7 §12.5.2	800-53 800-53A	422.501 495.346 21 CFR §11.1e §11.10d §11.10k	2.3- 2.4 7.1- 7.2 11.1- 11.3
Acquisition Development and Maintenance	Acquisition and Procurement Policy Application Implementation Policy Approved Application Policy Audit Trails Policy Change Management Policy Encryption Policy Hardware and Software Maintenance Patch Management Policy Production Input Output Controls Software Development Policy System Development Process Policy VPN Policy	§10.1.4 §12.3.2 §12.5.1 §12.5.2 §12.6.1	800-14 800-26 800-53A	495.348 820.50 820.80	2.1 2.2 3.5-3.6 4.1 6.1 – 6.6
Incident Management	Incident Response Policy Incident Response Plan Reporting Violations Policy	§A.13.2.1 §4.2.3 (b) §A.13.2.1 §A.13.1.1	800-53A IR-7 AC-2	422.128	11.4- 11.5 12.9
Business Continuity Management	Business Continuity Plan Business Continuity Policy Business Resumption Plan Continuity Communications Plan Dept Continuity of Operations Plan IS Disaster Recovery Plan	§A.14.1.1 §A.14.1.3 §A.14.1.1 §A.14.1.5 §A.14.1.5	800-14 800-53A	164.308	9.5 9.6
Compliance	Certification and Accreditation Policy Compliance Policy	§A.15.3.1 §A.15.1.4	800-14 800-34		6.4.5 10.6 11.2

### Standards

All organizations regardless of size need to secure their data and intellectual property. Information systems must be protected against unauthorized information disclosure (confidentiality), disruption (availability), and reliability (integrity).

Standards represent the knowledge of a large number of experts and provide security implementation recommendations. Each standard helps an organization address security related issues.

- *International Organization for Standardization (ISO)* - ISO is the world's largest developer and publisher of International Standards. ISO's globally accepted security standards ISO 27001 and 27002 are the defacto standards for information security.



## Altius IT Policy Collection Compliance and Standards Matrix

- *National Institute of Science and Technology (NIST)* - NIST develops and issues standards guidelines and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.
- *Federal Information and Information Systems Standards (FIPS)* - Federal agencies determine the security category of their information system in accordance with the provisions of FIPS 199 and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems.
- *Health (HIPAA, CFR, HITECH)* - Privacy and security rules provide guidelines for safeguarding the use and disclosure of certain confidential medical information known as Protected Health Information (PHI).
- *Payment Card Industry Data Security Standard (PCI DSS)* - PCI DSS helps prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold process or exchange cardholder information.

### **Relationships of security controls**

Altius IT's compliance matrix provides organizations with a general indication of security controls. In many cases the controls have similar but not exactly the same functionality. In some instances similar topics are addressed in the security control sets but provide a different context perspective or scope.

### **Compliance**

Please refer to the Matrix to see how Altius IT's Policy Collection ([www.AltiusIT.com/policies.htm](http://www.AltiusIT.com/policies.htm)) helps organizations meet information security standards and compliance requirements.