Altius IT Policy Collection Compliance and Standards Matrix

Security Controls	Altius IT Policy and Plan	ISO	NIST	Health	PCI	US, EU	COBIT
Governance Leadership Context	Context and Alignment Policy IT Governance Policy Mergers and Acquisitions Policy Terms and Definitions Policy	§4.1 – 4.4 §5.1 A.6.1.1 A.6.1.2	800-26 800-30 800-33 800-53 800-60 800-171	164.308	12.4 12.5		EDM01 EDM02 EDM03
Information Security	Clear Desk Policy EU Privacy and Data Protection Policy Privacy Policy Securing Information Systems Policy Security Controls Review Policy	§9.3 A.10.6 A.18.1	800-14 800-53 800-53A 800-171	422.112	12.1	European Union General Data Protection Regulation (GDPR)	APO13
Planning Risk Management	Business Impact Analysis Cybersecurity Policy Cybersecurity Framework Policy Risk Assessment Policy Risk Management Policy	§4.1 §6.1 §8.2 – 8.3 §9.3 §10.2 A.8.1.1	800-14 800-30 800-53 800-53A CSF Cyber	45 CFR §164.308 422.504 820.22	6.1-6.2 6.5 10.6 12.2	RA-1 RA-2 RA-3	APO12
Policies and Procedures	Security Policy Security Policy Intro System Security Plan	§5.2 §7.3 A.9.4.3	800-14 800-18 800-34 800-53 800-61 800-171	422.112 422.202	2.5 4.3 12.1 12.4-12.5	PM-10	DSS05
Organization	Audit Policy IT Management Policy Non-Disclosure Agreement Outsourcing Policy Staffing Policy	§5.3 §6.2 §9.2 – 9.3 A.5.1.1 A.6.1 A.7.1.1 – 2 A.7.2.3 A.9.2.6 A.12.7.1 A.13.2.4	800-48 800-53 800-53A 800-88 800-171	422.503 ARRA 13408 13404(b) 13405(b)	6.1 6.6 11.2-11.3 11.6	CA-1 CA-2 CA-8 PS-1	DSS06

Altius IT Policy Collection Compliance and Standards Matrix

Security Controls	Altius IT Policy and Plan	ISO	NIST	Health	PCI	US, EU	COBIT
Asset Management	Asset Management Policy Data Classification Policy Network Access Policy Software Licensing Policy	A.8.1 – 8.2 A.6.2.2 A.8.2 A.9	800-14 800-18 800-26 800-53 800-171	21 CFR 11.1(b) 11.1(f)	2.4 9.6-9.7 9.9 11.1 12.3	EU Dir PIPEDA	BAI09
Human Resources Communication	Acceptable Use Policy Audit Policy Security Awareness & Training Plan Security Awareness & Training Policy Staffing Policy Social Networking Security Policy Third Party Service Providers Policy	§7.2 – 7.4 A.5.1.1 A.5.1.2 A.7.2.2 A.8.1.3 A.13.2.2 A.15.1 – 2	800-14 800-26 800-50 800-53 800-171	21 CFR §820.20b §820.75b §820.25a PHIPA	2.6 8.5 12.6 12.8-12.9	AC-20 AT-1 AT-2 AT-3	APO07 APO08 APO09 APO10 BAI08
Physical Environmental	Facility Security Plan Personnel Security Policy Physical Access Security Policy Physical Security Policy	A.8.3.3 A.11.1.1 – 6 A.11.2.1 – 9	800-14 800-53	164.310	9.1-9.4 9.10 12.7	PE-1 PE-2 PE-3 PE-6	

Altius IT Policy Collection Compliance and Standards Matrix

Security Controls	Altius IT Policy and Plan	ISO	NIST	Health	PCI	US, EU	COBIT
Operation Support	Account Management Policy	§4.3	800-14	820-60	1.1-1.3	AU-2	BAI10
	Anti-Malware Policy	§5.2.e	800-41	820-65	1.5	AU-3	DSS01
	Backup Plan	§5.3.b	800-53		2.1	AU-6	MEA01
	Backup Policy	§6.1.2.c.1	800-53A		5.1-5.4	AU-7	
	Bluetooth Policy	§6.1.3	800-83		7.1-7.2	AU-8	
	Capacity and Utilization Policy	§7.2.d			8.2	AU-9	
	Data Integrity Policy	§7.5			8.5-8.7	CM-1	
	Data Marking Policy	§8.1			9.5-9.8	CM-2	
	Data Privacy Policy	§9.1			9.10	CM-6	
	Database Security Policy	§9.3.c			10.3-10.5	CM-7	
	Disposal Policy	A.7.3.1			10.8	CM-8	
	Documentation Policy	A.8.1.4				CP-9	
	Domain Controller Policy	A.8.2.2				MP-2	
	Domain Name System Policy	A.8.3.1 - 2				MP-4	
	E-commerce Policy	A.9.2				MP-6	
	E-mail Policy	A.10.1				SA-5	
	Firewall Policy	A.11.2.4				SC-2	
	Guess Access Policy	A.11.2.7				SC-4	
	Internet Connection Policy	A.12.1.1				SC-7	
	Intrusion Detection Policy	A.12.1.3				SC-8 (1)	
	Logging Policy	A.12.2				SC-13	
	Mass Communication Policy	A.12.3				SC-15	
	Network Address Policy	A.12.4				SC-28	
	Network Configuration Policy	A.12.5.1				SI-2	
	Network Documentation Policy	A.12.6.2				SI-3	
	Ransomware Policy	A.13.2				SI-4	
	Removable Media Policy	A.18.1.4					
	Router Security Policy						
	Security Monitoring Policy						
	Server Hardening Policy						
	Vendor Access Policy						
	Workstation Security Policy						

Altius IT Policy Collection Compliance and Standards Matrix

Security Controls	Altius IT Policy and Plan	ISO	NIST	Health	PCI	US, EU	COBIT
Access Control	Access Control Policy Admin Special Access Policy Bring Your Own Device Policy & Tech Guest Access Policy Identification and Authentication Logical Access Controls Policy Mobile Device Policy Password Policy Portable Computing Policy Remote Access Policy Securing Information Systems Policy Securing Sensitive Information Policy Smartphone Policy System Update Policy User Privilege Policy Wearable Computing Device Policy Web Site Policy Wireless Access Policy	A.6.2 A.7.3.1 A.9.1.1 – 2 A.9.2.4 A.9.3.1 A.9.4.1 A.9.4.2 A.9.4.3 A.13.1.1 – 3 EU Dir PIPEDA	800-48 800-53 800-53A 800-124 800-153 800-171	422.501 495.346 21 CFR §11.1e §11.10d §11.10k	1.4 3.2 4.1 7.3 8.1-8.4 8.8 11.1 11.4-11.5 12.3 A.1	AC-2 AC-3 (4) AC-4 AC-6 AC-7 AC-11 (1) AC-17 (2) AC-18 (1) AC-19 AC-20 (1) AC-20 (2) AC-22 IA-1 IA-2 IA-4 IA-5 (1)	MEA02
Acquisition Development Maintenance	Acquisition and Procurement Policy Application Implementation Policy Approved Application Policy Audit Trails Policy Change Management Policy Encryption Policy Green Computing Policy Hardware and Software Maintenance Patch Management Policy Production Input Output Controls Quality Assurance Policy Secure Development Lifecycle Policy Server Certificates Policy Software Development Policy VPN Policy Web Site Policy	§6.2 §7.1 §9.1 §9.3 §10.2 A.9.4.5 A.10.1 – 2 A.11.2.4 A.12.1.2 A12.1.4 A.12.6.1 A.13.2 A.14.1 A.14.2 A.14.3.1	800-14 800-26 800-40 800-53 800-53A 800-64	495.348 820.50 820.80	2.2-2.3 3.5-3.7 4.1 6.2-6.7 10.1-10.2 10.6-10.7	MA-4 (6) MA-5 MA-6 RA-5	BAI03 BAI06 BAI07

Altius IT Policy Collection Compliance and Standards Matrix

Security Controls	Altius IT Policy and Plan	ISO	NIST	Health	PCI	Federal	COBIT
Incident Management	Identity Theft Protection Policy Incident Response Policy Incident Response Plan Reporting Violations Policy	§9.3.c §10.1 A.16.1	800-53 800-61 IR-7 AC-2	422.128 ARRA 13402	11.1 12.5 12.10	IR-2 IR-4 IR-5 IR-6	BAI09 DSS02 DSS03
Business Continuity Disaster Recovery	Business Continuity Plan Business Continuity Policy Business Resumption Plan Continuity Communications Plan Dept Continuity of Operations Plan IS Disaster Recovery Plan	A.17.1 A.17.2 A.11.1.4	800-14 800-34 800-53	164.308	9.5 12.10	CP-4 CP-5 CP-7 CP-10 SA-14	BAI04 DSS04
Compliance Performance Evaluation	Business Associates Agreement Certification and Accreditation Policy Compliance Policy Data Retention Policy HIPAA and HITECH Policy PCI Policy Security Controls Review Policy	A.7.1.2 A.8.1.4 A.13.1.2 A.13.2.2 A.13.2.4 A.18.1 A.18.2 EU Dir PIPEDA	800-14 800-34 800-53A 800-66 800-122	ARRA 13405(a) PHIPA	1.1 3.1-3.4 3.7 4.2 9.9	SI-12	MEA03

Altius IT Policy Collection Compliance and Standards Matrix

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.

- *Control Objectives for Information and Technology (COBIT)* - COBIT 5 is a framework created by the Information Systems Audit and Control Association (ISACA) for information technology governance and management. COBIT is a strategic management tool developed with the help of world-wide experts in the field of IT governance, IT management, performance management, and information security and control. The Altius IT Policy Collection helps organizations meet COBIT information security and control requirements.
- *European Union (GDPR General Data Protection Regulation).* Privacy and security policies and procedures governing the collection, use, or disclosure of Sensitive Information.
- *International (ISO, PIPEDA, EU Directive).* The International Organization for Standardization (ISO) is the world's largest developer and publisher of International Standards. ISO's globally accepted security standards ISO 27001 and 27002 are the de facto standards for information security. In addition to ISO, the protection of personal data is governed by Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the EU Directive on the Protection of Personal Data, and United Kingdom's Data Protection Act of 1998 (adopts the EU Directive).
- *National Institute of Science and Technology (NIST)* - NIST develops and issues standards guidelines and other publications to assist organizations in implementing the Federal Information Security Management Act (FISMA) of 2002, the 2014 Framework for Improving Critical Infrastructure Cybersecurity (CSF Cybersecurity Framework), and cost effective programs to protect 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. European Union Data Protection Regulation (GDPR) requirements.

- *Federal Register Vol. 79, No. 222 Minimum Security Controls* - minimum required security controls for unclassified controlled technical information requiring safeguarding. A description of the security controls is in NIST SP 800–53, ‘‘Security and Privacy Controls for Federal Information Systems and Organizations’’.
- *Health (HIPAA, CFR, HITECH, Canada Personal Health Information Protection Act PHIPA)* - Privacy and security rules provide guidelines for safeguarding the use and disclosure of certain confidential medical information known as Protected Health Information (PHI). Specifies data breach disclosure requirements.
- *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 store, 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) helps organizations meet information security standards and compliance requirements.