



Policy Coverage Matrix for ISO 17799:2005*

Information Security Policies Made Easy, Version 10.0

This table maps the high-level security control requirements of the ISO 17799:2995 Standard and the information security policies found within ISPME V10. ISPME policies are organized around the ISO 17799:2000 standard, but still provide topic coverage for the new standard. Areas of significant change are marked in blue.

ISO 17799:2005 Security Control Topics	ISPME Specific Sections and Policies
5 SECURITY POLICY 5.1 INFORMATION SECURITY POLICY	3 SECURITY POLICY 3.1 Information Security Policy
6 ORGANIZATION OF INFORMATION SECURITY 6.1 INTERNAL ORGANIZATION 6.2 EXTERNAL PARTIES	4 ORGANIZATIONAL SECURITY 4.01 Information Security Infrastructure 4.02 Security Of Third-Party Access 4.03 Outsourcing
7 ASSET MANAGEMENT 7.1 RESPONSIBILITY FOR ASSETS. 7.2 INFORMATION CLASSIFICATION	5 ASSET CLASSIFICATION AND CONTROL 5.01 Accountability For Assets 5.02 Information Classification
8 HUMAN RESOURCES SECURITY 8.1 PRIOR TO EMPLOYMENT 8.2 DURING EMPLOYMENT 8.3 TERMINATION OR CHANGE OF EMPLOYMENT	6 PERSONNEL 6.01 Security In Job Definition And Resourcing 6.02 User Training 6.03.05 <i>Disciplinary Process</i>
9 PHYSICAL AND ENVIRONMENTAL SECURITY 9.1 SECURE AREAS 9.2 EQUIPMENT SECURITY	7 PHYSICAL AND ENVIRONMENTAL SECURITY 7.01 Secure Areas 7.02 Equipment Security 7.03 <i>General Controls (put into 9.1 and 9.2)</i>
10 COMMUNICATIONS AND OPERATIONS MANAGEMENT 10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT 10.3 SYSTEM PLANNING AND ACCEPTANCE. 10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE 10.5 BACK-UP 10.6 NETWORK SECURITY MANAGEMENT 10.7 MEDIA HANDLING . 10.8 EXCHANGE OF INFORMATION 10.9 ELECTRONIC COMMERCE SERVICES 10.10 MONITORING	8 COMMUNICATIONS AND OPERATIONS MANAGEMENT 8.01 Operational Procedures And Responsibilities 4.02 <i>Security Of Third-Party Access</i> 8.02 System Planning And Acceptance 8.03 Protection Against Malicious Software 8.04 Housekeeping (8.04.01 Information Backup) 8.05 Network Controls 8.06 Media Handling and Security 8.07 Exchanges Of Information And Software 8.07.03 <i>Electronic Commerce Security</i> 9.07 <i>Monitoring System Access And Use</i>

<p>11 ACCESS CONTROL</p> <p>11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL 11.2 USER ACCESS MANAGEMENT. 11.3 USER RESPONSIBILITIES 11.4 NETWORK ACCESS CONTROL. 11.5 OPERATING SYSTEM ACCESS CONTROL 11.6 APPLICATION AND INFORMATION ACCESS CONTROL 11.7 MOBILE COMPUTING AND TELEWORKING</p>	<p>9 ACCESS CONTROL</p> <p>9.01 Business Requirement For Access Control 9.02 User Access Management 9.03 User Responsibilities 9.04 Network Access Control 9.05 Operating System Access Control 9.06 Application Access Control 9.08 Mobile Computing</p>
<p>12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE</p> <p>12.1 SECURITY REQUIREMENTS OF INFO SYSTEMS 12.2 CORRECT PROCESSING IN APPLICATIONS 12.3 CRYPTOGRAPHIC CONTROLS 12.4 SECURITY OF SYSTEM FILES 12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES 12.6 TECHNICAL VULNERABILITY MANAGEMENT</p>	<p>10 SYSTEMS DEVELOPMENT AND MAINTENANCE</p> <p>10.01 Security Requirements Of Systems 10.02 Security In Application Systems 10.03 Cryptographic Controls 10.04 Security Of System Files 10.05 Security In Development And Support Processes NA</p>
<p>13 INFORMATION SECURITY INCIDENT MANAGEMENT</p> <p>13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES. 13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS</p>	<p>6.03 Responding To Security Incidents And Malfunctions</p> <p>6.03.01 Reporting Security Incidents 6.03.02 Reporting Security Weaknesses 6.03.03 Reporting Software Malfunctions 6.03.04 Learning From Incidents</p>
<p>14 BUSINESS CONTINUITY MANAGEMENT</p> <p>14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT</p>	<p>11 BUSINESS CONTINUITY MANAGEMENT</p> <p>11.01 Aspects Of Business Continuity Management</p>
<p>15 COMPLIANCE</p> <p>15.1 COMPLIANCE WITH LEGAL REQUIREMENTS 15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE 15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS</p>	<p>12 COMPLIANCE</p> <p>12.01 Compliance With Legal Requirements 12.02 Reviews Of Security Policy And Technical Compliance 12.03 System Audit Considerations</p>

**Information based on ISO 17799:2005 Code of practice for information security management, released in July, 2005.*

*** Notes: Changes in the ISO numbering scheme have created an offset between ISPME section numbers and ISO categories. Differences in organization and numbering are [highlighted in blue](#).*