MA 201 CMR 17.00 Policy Mapping Table

The following table illustrates how the security policy topic categories of *Information Security Policies Made Easy* (ISO 27002) map to the specific high-level control requirements outlined in the Massachusetts state data protection law known as 201 CMR 17. [1]

Specific Program Requirements	ISO Category
17.03 Duty to Protect and Standards for Protecting Personal Information	(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards
1.0 Protection Requirements *Identification of customer PII requires a data classification program.*	7.2.1 Classification guidelines 7.2.2 Information labeling and handling 6.2.2 Addressing security when dealing with customers *(Sample Information Classification Policy)*
2. Written Security Program Requirements *Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:*	6.1.1 Management commitment to information security 6.1.2 Information security co-ordination *(Sample Security Program Policy)*
(a) Assigned Security Responsibility *(a) Designating one or more employees to maintain the comprehensive information security program;*	6.1.3 Allocation Of Information Security Responsibilities *(Sample Security Program Policy)*
(b) Ongoing Risk Assessment *Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:* *1. ongoing employee (including temporary and contract employee) training;* *2. employee compliance with policies and procedures; and* *3. means for detecting and preventing security system failures.*	6.1.2 Information Security Coordination 6.1.1- 2. Risk Assessments 6.2.1 Identification of risks related to external parties 14.1.2 Business continuity and risk assessment 15.1.1- 6. System Risk Assessments *(Sample IT Risk Assessment Policy)*
(c) Written Acceptable Use Security Policies *Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.*	5.1.1 Information Security Policy Document 7.1.1 Acceptable Use of Assets *(Acceptable Use of Assets Policy)*
(d) Employee Sanctions *Imposing disciplinary measures for violations of the comprehensive information security program rules.*	8.2 DURING EMPLOYMENT 8.2.3 Disciplinary process
(e) Employee termination procedures *Preventing terminated employees from accessing records containing personal information.*	8.3 TERMINATION OR CHANGE OF EMPLOYMENT 8.3.1 Termination responsibilities 8.3.2 Return of assets 8.3.3 Removal of access rights
(f) Service Provider Oversight *Oversee service providers, by:*	6.2 EXTERNAL PARTIES

Specific Control Objectives	ISO Category
(f-1)Service Provide Risk Assessment *Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and*	6.2.1 Identification of risks related to external parties *(Sample Third Party Security Policy)*
(f-2)Service Provider Contract Requirements *Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information;*	6.2.3 Addressing security in third party agreements *(Sample Third Party Security Policy)*
(g) Physical Security Controls *Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.*	9 PHYSICAL AND ENVIRONMENTAL SECURITY 9.1 SECURE AREAS 9.2 EQUIPMENT SECURITY *(Sample Physical Security Policy)*
(h) Security Program Monitoring *Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.*	15.2.1 Compliance with security policies and standards. 15.2.2 Technical compliance checking
(i) Annual Security Program Review *Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.*	6.1.8 Independent review of information security 5.1.2 Review of the information security policy *(Sample Security Program Policy)*
(j) Incident Response Management *Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.*	13 INFORMATION SECURITY INCIDENT MANAGEMENT 13.1.1 Reporting information security events 13.1.2 Reporting security weaknesses *(Sample Incident Response Policy)*
17.04: Computer System Security Requirements	Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.
1. Identification and Authentication *Secure user authentication protocols including:*	11.2 USER ACCESS MANAGEMENT 11.3 USER RESPONSIBILITIES 11.3.1 Password use. 11.5.1 Secure log-on procedures 11.5.2 User identification and authentication
a. User ID Management *control of user IDs and other identifiers;*	11.2.1 User registration 11.2.2 Privilege management *(Sample Account Management Policy)*
b. Secure Password Selection *a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;*	11.2.3 User password management *(Sample Password Management Policy)*
c. Password Protection *control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;*	11.3.2 Unattended user equipment 11.3.3 Clear desk and clear screen policy *(Sample Acceptable Use of Assets Policy)*
d. User Account Restrictions (expiration) *restricting access to active users and active user*	11.2.4 Review of user access rights *(Sample Account Management Policy)*

Specific Control Objectives	ISO Category
accounts only; and	
e. Max login attempts *blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;*	11.3.2 Unattended user equipment 11.5 Operating System Access Control *(Sample Access Control Policy)*
2. Access Controls *Secure access control measures that:*	11 ACCESS CONTROL 11.1.1 Access control policy 11.2 User Access Management 11.4 Network Access Control 11.5 Operating System Access Control 11.6 Application and Information Access Control *(Sample Access Control Policy)*
a. Privilege Restriction - Need to Know *restrict access to records and files containing personal information to those who need such information to perform their job duties; and*	11.2.2 Privilege management *(Sample Access Control Policy)*
b. Unique UserID and Passwords *assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;*	11.2.3 User password management 11.3.1 Password use (*Sample Password Management Policy)* *(Sample Account Management Policy)*
c. Change Vendor Default Passwords *not vendor supplied default passwords,*	10.3.2 System acceptance (*Sample Password Management Policy)*
3. Transmission Protection of PII *Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.*	10.7.3 Information handling procedures 10.8.1 Information exchange policies and procedures 10.8.2 Exchange agreements 10.8.3 Physical media in transit 10.8.4 Electronic messaging *(Information Exchange Policy)* *(Acceptable Use of Email Policy)*
4. Systems Monitoring *Reasonable monitoring of systems, for unauthorized use of or access to personal information.*	10.10 MONITORING 10.10.1 Audit logging 10.10.2 Monitoring system use 10.10.3 Protection of log information 10.10.4 Administrator and operator logs 10.10.5 Fault logging *(Sample Log and Audit Management Policy)*
5. Portable Device Encryption *Encryption of all personal information stored on laptops or other portable devices;*	11.7.1 Mobile computing and communications 11.7.2 Teleworking *(Sample Mobile Security Management Policy)*
6. Network Security *For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.*	11.4 NETWORK ACCESS CONTROL 10.6 NETWORK SECURITY MANAGEMENT 10.6.1 Network controls 10.6.2 Security of network services *(Sample Network Security Management Policy)*
6.1 Firewalls *, there must be reasonably up-to-date firewall protection and*	11.4.6 Network connection control 11.4.7 Network routing control *(Sample Firewall Policy)*
6.2 Updated OS Patching *[…] operating system security patches, reasonably designed to maintain the integrity of the personal information.*	10.1.2 Change management 12.6.1 Control of technical vulnerabilities

7. Malicious Software Protection *Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions,*	10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE *(Sample Malicious Software Policy)*
8. Employee Education and Training *People are a crucial factor in ensuring the security of computer systems and valuable information resources.*	8.2.2 Information security awareness, education, and training *(Sample Personnel Security Policy)*
17.05: Compliance Deadline	*(1)Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.*

References:

[1] 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

[2] ISO/IEC 17799:2005 (ISO 27002) – Code of practice for information security management - Published by ISO and available at BSI [http://www.bsi-global.org/]

*Note: The policies within the ISPME follow the topic categories of the ISO 27002 outline.