

201 CMR 17.00: Compliance Readiness

We recommend that you complete the following two (2) tables to determine if you have a problem achieving compliance with 201 CMR 17.00

How Ready is Your Company for 201 CMR 17.00 Compliance?	Your Situation
Number of customers, clients, or accounts that contain personal identity information (PII)?	
Do you use 3 rd -party service providers who have access to or use of your personal identity information (PII)? (How many?)	
Do you have in house IT resources? (Yes, No, Somewhat)	
Do you have in house HR resources? (Yes, No, Somewhat)	
Do you have a policy and procedures manual for employees that incorporates provisions for preventing unauthorized access to or use of consumer and personal identity information (PII)?(Yes, No, Somewhat)	
Do you have employee job descriptions? (Yes, No, Somewhat)	
Do you have a written information security program (ISP) that includes provisions for preventing unauthorized access to or use of consumer and personal identity information (PII)? (Yes, No , Somewhat)	
If you have an information security program (ISP), is it 201 CMR 17.00 compliant? (Yes, No, Somewhat)	
Do you have on board expertise in writing security policies and procedures? (Yes, No, Somewhat)	
Do you have on board expertise for implementing the technologies required to comply with 201 CMR 17.00? (Yes, No, Somewhat) <ul style="list-style-type: none"> • Encryption • Intrusion Detection 	

You now have a high level overview of what 201 CMR 17.00 will require of your company. Go to the next table and assess your needs for the assigning the right job skills to develop your comprehensive, written information security program.

- Will you need to hire IT expertise?
- Do you have an employee who can competently maintain Your WISP?



Job Skills Needed for Complying with 201 CMR 17.00 Regulations

Complete the following table(s) to assess your ability to develop and implement a comprehensive written information security program (WISP) using on board staff versus hiring expensive third-party IT consultants.

The job related skills you need to develop Your WISP fall into the following broad categories.

- If appropriate, the ability to write a job description for your designated information security coordinator (ISC).
- Ability to write or amend employee agreements or information security policies and procedures.
- Ability to implement the technologies necessary to support your policies and to conform to the regulations.

Policy column of the table(s):

- If marked with a “Y”, it means that the guidebook includes a sample policy, procedure or other document to assist you in complying with this section of the regulation.
- If marked “N/A” or left “blank”, means the guidebook does not provide a sample policy, procedure or other document to assist you in complying with this section of the regulation

Section 17.03: Duty to Protect and Standards for Protecting Personal Information

201 CMR 17.00 Section	Job Skills Needed for Complying with 201 CMR 17.00 Regulations	Have This Skill	Policy
17.03: (2) (a)	Requires you to designate an employee to maintain Your WISP. <ul style="list-style-type: none"> • Better compliance is to write or amend an Information Security Coordinator (ISC) job description. 		Y
17.03: (2) (b)	Requires you to perform a “risk based” analysis of reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI and, if necessary, improving the effectiveness of the current safeguards for limiting such risks.		Y
17.03: (2) (c)	Requires you to develop security policies for employees relating to the storage, access and transportation of records containing PI outside of business premises.		Y



201 CMR 17.00 Section	Job Skills Needed for Complying with 201 CMR 17.00 Regulations	Have This Skill	Policy
	<p><u>DEVELOP OR AMEND EMPLOYEE AGREEMENT(S), SUCH AS:</u></p> <ul style="list-style-type: none"> • Standard Employee Agreement • Employee Non-Disclosure Agreement • Employee Confidentiality Agreement • (Independent Contractor) Confidentiality Agreement <p><u>TO COMPLY WITH THE REGULATIONS FOR:</u></p>		Y
17.03: (2) (d)	<ul style="list-style-type: none"> • Imposing disciplinary measures for violating WISP rules 		Y
17.03: (2) (e)	<ul style="list-style-type: none"> • Preventing terminated employees from accessing personal information (PI) 		Y
	Overseeing Third-Party Service Providers		
17.03: (2) (f)	<p>Requires you to oversee third-party service providers</p> <ul style="list-style-type: none"> • Review and amend your contracts for conformance with 201 CMR 17.00. • Assure third-party service provider compliance with 201 CMR 17.00. 		Y
	<u>Writing or Amending Policies and Implementing Best Practices for:</u>		
17.03: (2) (g)	<ul style="list-style-type: none"> • Reasonably restricting physical access to personal identity information. 		Y
17.03: (2) (g)	<ul style="list-style-type: none"> • Implementing this policy for storage of records containing PI in locked facilities, storage areas or containers. 		
17.03: (2) (h)	<p>Monitoring Your WISP to ensure that it is operating as designed to prevent unauthorized access to or use of personal identity information and improving its effectiveness where necessary.</p>		Y
17.03: (2) (i)	<p>Writing or amending and implementing a policy for:</p> <ul style="list-style-type: none"> • Reviewing Your WISP, at least annually, for a material change in business practice that might impact the integrity of your PI 		Y
17.03: (2) (j)	<p>Writing or amending and implementing policies, procedures and best practices for efficient response to security breaches of personal identity information.</p>		Y



Section 17.04: Computer Systems Security

201 CMR 17.00 Section	Job Skills Needed for Complying with 201 CMR 17.00 Regulations	Have This Skill	Policy
	Implementing and Documenting Computer Systems Security for Complying with Section 17.04, including:		
	Secure User Authentication Protocols:		Y
17.04: (1) (a)	<ul style="list-style-type: none"> Control of user IDs and other identifiers. 		
17.04: (1) (a)	<ul style="list-style-type: none"> Control of user IDs and other identifiers. 		
17.04: (1) (b)	<ul style="list-style-type: none"> A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices. 		
17.04: (1) (c)	<ul style="list-style-type: none"> 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. 		
17.04: (1) (d)	<ul style="list-style-type: none"> Restricting access to active users and active user accounts only. 		
17.04: (1) (e)	<ul style="list-style-type: none"> Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system. 		
	Secure Access Control Measures that:		N/A
17.04: (2) (a)	<ul style="list-style-type: none"> Restrict access to records containing PI to those who need such information to perform their job duties. 		
17.04: (2) (b)	<ul style="list-style-type: none"> 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. 		
17.04: (3)	Encrypting all PI transmitted over public networks.		Y
17.04: (3)	Encrypting PI to be transmitted wirelessly.		Y
17.04: (4)	Reasonable monitoring of systems for unauthorized use of PI.		Y
17.04: (5)	Encrypting all PI on stored on laptops and other portable devices.		Y
17.04: (6)	Maintaining reasonably up-to-date firewall and operating system protection for all systems connected to the internet.		Y
17.04: (7)	Maintaining reasonably up-to-date versions of security agent software which must include malware and virus protection.		Y
17.04: (8)	Educating and training employees in the; proper use of the computer security system and importance of protecting personal information.		Y

So that's it. How did your company stand up to the requirements of 201 CMR 17.00? Are you ready to comply?





Don't Panic - We've Got You Covered!

A large number of NO (N) responses in column 4 (Have This Skill) is an indication of how much of Your WISP needs to be developed using third-party IT consultants. This guidebook greatly reduces your need for hiring expensive consulting resources by including

1. Sample job descriptions, policies, procedures and best practices that you can modify to fit your circumstances.
2. Links to expert websites that provide guidance on
 - How to write policies or procedures
 - Best practices for protecting consumer and personal information from identity theft and fraud
3. Links to websites that provide “free” samples and templates of technical security policies and procedures for inclusion in your written information security program (WISP).
4. Reasonable action for compliance, best practice(s) and processes for implementing the technology required by the regulation.
5. Timely Tips from the Federal Trade Commission.

