NDIS IT/Information Security
Examination Workprogram

201 CMR 17.00 REFERENCE	WORK PROGRAM STEP #	EXAMINATION PROCEDURE	EXAMINATION GUIDANCE	YES	NO	VIO	EXAMINATION COMMENTS
GENERAL							
	1	Review and assess the overall information provided by the Licensee in the IT Officer's Questionnaire	*Assess overall content for completeness, expanded information as needed, blank spaces or missing information/documents, etc. When completing the IT program examiner(s) should consider the size and complexity of the Licensee relative to its IT operations.*				
I. RISK ASSESSMENT AND MANAGEMENT OVERSIGHT							
		Risk Assessment					
17.03(2)(b)	2	Has the Licensee given consideration to IT matters when formulating its overall business strategy?	*Management should consider IT and information security risk when making business decisions.*				
17.03(2)(b)	3	Has the Licensee established an IT risk assessment program and performed an IT risk assessment?	*Licensees must perform a risk assessment of security risks to both paper and electronic systems containing personal information which identifies reasonable, foreseeable security risks (both internal and external) and the potential damage those risks can cause. Failure to establish a risk assessment program is a violation of 201 CMR 17.03(2)(b).*				
	4	When was the last IT risk assessment performed?					
II. WRITTEN INFORMATION SECURITY PROGRAM (WISP)							
17.03 and 17.04	5	Does the Licensee have a Written Information Security Plan (WISP)?	*Licensees must develop, implement and maintain a WISP which provides safeguards for the protection of consumer personal information. Failure to maintain a WISP is a violation of 201 CMR 17.03.*				
17.03(2)(a)	6	Does the Licensee designate one or more individuals who will oversee and maintain the WISP?					
17.03(2)(h) and (i)	7	Does the Licensee review and upgrade its WISP at least annually?					
17.03(2)(c)	8	Does the Licensee have any other IT policies and procedures?	*In addition to the WISP. A WISP alone may not be adequate for large and complex companies. May need additional policies including Vendor Management Policies*				
17.03(2)(b)1. and 2. & 17.04(8)	9	Are IT policies and procedures disseminated to all staff as appropriate?	*(User Access Policy)*				

NDIS IT/Information Security
Examination Workprogram

201 CMR 17.00 REFERENCE	WORK PROGRAM STEP #	EXAMINATION PROCEDURE	EXAMINATION GUIDANCE	YES	NO	VIO	EXAMINATION COMMENTS
II. WRITTEN INFORMATION SECURITY PROGRAM (WISP) - Continued							
17.03(2)(j) and MGL c. 93 H	10	Has the Licensee experienced a systems security breach to date?	*Licensees are required to follow the requirements outlined in MGL chapter 93H if they have experienced a data breach. Failure to report a data breach is a violation of M.G.L. chapter 93H, section 3.*				
III. DATA SECURITY OPERATIONS							
		Access Controls					
17.03 (2)(e) & 17.04 (1)(d)	11	Does the Licensee place access restrictions when users permanently leave employment, are terminated, or are absent for an extended period of time?	*Example: A Licensee's IT dept. should receive immediate notification from HRD and take prompt action to delete/disable user IDs*				
17.04(2)(a)	12	Does the Licensee place limitations on access controls to ensure that users can only access data related to their specific job duties?	*Licensees should be able to generate a report to demonstrate appropriate access levels based on job functions.*				
		User IDs and Passwords					
17.04(1)(b)	13	Does each employee have a unique password with minimum complexity requirements?					
17.04(1)(e)	14	Does the Licensee block access to user identification after multiple unsuccessful logon and/or password attempts?					
		Third Party Service Providers					
17.03(2)(f)1. and 2.	15	Has the Licensee identified the third party service providers they share sensitive and personal consumer information with?					
17.03 (2)(F)(1)	16	Does the licensee conduct adequate initial due dilligence prior to engaging a 3rd party service provider?					
17.03(2)(f)2.	17	Are these service providers required to confirm in writing that they adhere to the requirements of *201 CMR 17.00 et seq* ?	*Review a sample of third-party service provider agreements to ensure that language to protect and safeguard personal information is included. Licensee should also monitor 3rd parties to ensure ongoing compliance.*				
17.03(2)(b)	18	Does the licensee risk rank (risk assess) to ensure ongoing monitoring of critical vendors?	Does the licensee conduct ongoing monitoring of critical vendors? [e.g. Does the Licensee risk rank (risk assess) so that they can conduct more robust ongoing monitoring of the more critical vendors (the vendors that they risk rated higher risk)]				

NDIS IT/Information Security
Examination Workprogram

201 CMR 17.00 REFERENCE	WORK PROGRAM STEP #	EXAMINATION PROCEDURE	EXAMINATION GUIDANCE	YES	NO	VIO	EXAMINATION COMMENTS
III. DATA SECURITY OPERATIONS - Continued							
		Training					
17.03(2)(b)1. & 17.04(8)	19	Does management provide on-going IT training specific to the safeguarding and integrity of consumer personal information?	*IT education and training for all employees must be ongoing and address the proper use of security computer systems and the importance of safeguarding consumer personal information.*				
		Monitoring					
17.03(2)(h) & 17.04(4)	20	Does the Licensee monitor/review its IT systems for unauthorized access and/or suspicious or malicious activity?	*Regular IT systems monitoring minimizes the possibility of unauthorized and/or malicious activity going undetected for extended periods of time and helps maintain acceptable use practices. Areas to be monitored include: firewall security reporting from 3rd party service providers; bad password attempts for user logons; time of day logon restrictions; VPN reports; intrusion detection (as applicable), etc.*				
		Network Security					
17.04(3)(5) and(8)	21	How does management handle the storing and transmittal of consumer personal information electronically? Is it encrypted and/or password protected? Are employees properly trained on system security and the importance of personal information security?					
17.04(6) & 17.04(7)	22	Are the Licensee's firewall protections and operating systems security patches, anti-virus and malware up-to-date?					
17.03(2)(c) & 17.04(3) and (5)	23	Do users have remote access to company servers? Is VPN used for encryption? Is remote access provided from a company-issued devices?	*i.e. access from home.*				
	24	Do consumers have the ability to access information, upload documents or manage their accounts online?					

NDIS IT/Information Security
Examination Workprogram

201 CMR 17.00 REFERENCE	WORK PROGRAM STEP #	EXAMINATION PROCEDURE	EXAMINATION GUIDANCE	YES	NO	VIO	EXAMINATION COMMENTS
III. DATA SECURITY OPERATIONS - Continued							
		Physical Security					
17.03(2)(g)	25	Are controls in place to ensure that only authorized personnel are permitted in areas with network file server(s), mainframes, or other significant hardware devices?	*Physical security includes: access to servers, desktop and laptop PCs and other network equipment and/or wireless devices, as well as, paper records to prevent unauthorized disclosure of consumer personal information.*				
17.03(1)(c)	26	Are fire detection and suppression devices in place? Are non-water based fire extinguishers in place?	*Best disaster recovery and business continuity related practices: i.e. FM200 (removes oxygen and cools the fire); carbon dioxide extinguishers; and/or dry chemical fire extinguishers.*				
17.03(1)(c)	27	Is an uninterruptible power supply (UPS) surge protection system for critical equipment in place?	*Licensees should test the UPS protection system on at least an annual basis.*				
17.03(2)(g)	28	How does the Licensee dispose of confidential information, including paper and electronic records and equipment?	*Paper should be shredded and electronic records should be purged pursuant to record retention requirements. As equipment is retired it should be inventoried and cleared of confidential information to ensure that it does not leave the Licensee containing confidential data.*				
IV. BUSINESS CONTINUITY AND DISASTER RECOVERY							
	29	Does the Licensee have a Business Continuity and Disaster Recovery Plan?	*Disaster Recovery plans should be in place to ensure that the Licensee can resume business in the event of a disaster/emergency or other unforeseen circumstance in a timely manner. Plan should: 1. include contact information 2. be reviewed at least annually 3. be appropriate for the size and complexity of the institution 4. be provided to employees.*				
17.03(2)(c) & (d)	30	Does the Licensee have response procedures for unauthorized access/use of personal information or malicious activity by employees?	*Compliance with 17.03(2)(c) and (d) requires that the Licensee develop and implement proper security policies for employees (i.e. Acceptable-Use policy) which would impose disciplinary measures for violations of WISP rules. Unacceptable or inappropriate use could lead to virus attacks; compromise of network systems and/or services; as well as legal issues.*				
17.03 (2)(j)	31	Does the Licensee have response procedures in place in the event that internal and/or external unauthorized or malicious activity does occur?					

NDIS IT/Information Security
Examination Workprogram

201 CMR 17.00 REFERENCE	WORK PROGRAM STEP #	EXAMINATION PROCEDURE	EXAMINATION GUIDANCE	YES	NO	VIO	EXAMINATION COMMENTS
V. CYBER-SECURITY							
	32	What security measures does licensee have in place to prevent cyber-attacks via these connections?	*For example: firewalls; anti-virus; passwords; encryption; etc.*				
	33	How does the Licensee keep up to date with existing and developing cybersecurity risks?	*Is cyber security risk incorporated into the licensee's training program?*				
	34	Does the licensee have a system in place to detect cyber-attacks and security breaches?	*In addition to detecting breaches, a licensee should be prepared to respond to those attacks, mitigate the damage posed by these attacks, escalate issues to senior management/board level as appropriate, report these incidents to customers, regulators & law enforcement, and continue business operations.*				
VI. IT AUDIT							
	35	Does the Licensee engage an internal and/or external IT auditor? Provide name(s) and title(s).	*IT audits are not required by the regulation. Most smaller Licensees may not have IT audits conducted. However, larger, more complex companies should have IT reviewed as part of their compliance audit program.*				
VII. EXAMINATION SUMMARY							
Examiner(s) should present and discuss preliminary findings and potential violations with the Licensee both before and during the examination exit conference. Examiner(s) should obtain and document Licensee management's commitment to address all issues determined in the examination. Examination findings, comments and conclusions, as well as, recommendations for corrective action should be summarized below.							

NDIS IT/Information Security
Examination Workprogram

VIII. EXAMINATION RESOURCE INFORMATION

201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth: www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

NDIS IT Compliance Guidelines for 201 CMR 17.00

FFIEC - Interagency Guidelines Establishing Information Security Standards

FFIEC IT Examination Handbooks: http://ithandbook.ffiec.gov/it-booklets.aspx

FFIEC Cybersecurity: www.ffiec.gov/cybersecurity.htm

CSBS best practices: http://www.csbs.org/ec/cato/Pages/cato.aspx

Office of Consumer Affairs and Business Regulations- 201 CMR 17.00 Compliance Checklist: http://www.mass.gov/ocabr/data-privacy-and-security/data/

FIL-68-2001 - Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information

FIL-9-2015 - Business Continuity Planning Booklet Appendix J Update to FFIEC IT Examination Handbook Series

http://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

IX. REGULATORY AUTHORITY

201 CMR 17.00
M.G.L. c. 93H
Gramm-Leach-Bliley Act (GLBA) - Safeguards Rule
FTC's Safeguarding Rule - 16 CFR 314

MASSACHUSETTS DIVISION OF BANKS
NON-DEPOSITORY INSTITUTION SUPERVISION
INFORMATION TECHNOLOGY OFFICER'S QUESTIONNAIRE

Instructions for Completing the Information Technology Officer's Questionnaire

Please provide detail information as attachments referencing sections and questions numbers where applicable.

The Information Technology Officer's Questionnaire (Questionnaire) contains questions covering significant areas of the Licensee's information technology (IT) function. Your responses to these questions will help determine the scope of the examination; provide insight into the composition of the Licensee's IT operations, information security program, and IT governance processes; and may be relied upon to form conclusions as to the condition of the Licensee's IT functions. Therefore, accurate and timely completion of the IT Questionnaire is expected. Examiners may request additional supporting documentation to assess the validity of the answers that are provided and to further assess the quality and content of the Licensee's IT operations and information security and IT governance programs.

The majority of the questions require a "Yes" or "No" response; however, you are encouraged to expand or clarify any responses, as needed, in the space below each question or at the end of this document under the heading "Additional Comments." For any question deemed non-applicable to your institution or if the answer is "None," please respond accordingly ("NA" or "None"). Please do not leave blank responses.

The Questionnaire concludes with an Information Technology Questionnaire Certification, which must be signed by an executive officer attesting to the accuracy and completeness of all information provided.

Question #	QUESTION	YES	NO	N/A	RESPONSE / COMMENTS
1	Please provide the name and title(s) for the individual(s) responsible for managing IT functions in your organizations.				
2	Do you electronically store consumer personal information, including but not limited to, social security numbers, financial statements, credit reports, bank statements and credit card?				
3	Have you performed a risk assessment of security risks to systems (both paper and electronic) containing personal information which identifies reasonable, foreseeable security risks (both internal and external) and the potential damage those risks can cause?				
3(a)	If yes, please provide a copy of your written risk assessment.				
3(b)	If yes, is your risk assessment program reviewed and updated annually?				
4	Do you have a comprehensive written information security program (WISP) designed to: ensure the security and protection of consumer personal information; protect against anticipated threats or hazards to the security or integrity of such information which may result in substantial harm or inconvenience to consumers?				
4(a)	If yes, please provide a copy of your WISP and indicate the last date it was updated?				
5	Does your WISP define and restrict access to servers and IT assets?				
6	Does your WISP incorporate dual control procedures, segregation of duties and employee background checks for employees with responsibilities for, or access to, consumer personal information?				
7	Do you have policies and procedures in place to ensure that critical updates for operating systems, databases, and software applications are applied?				
8	What security measures have you put in place to prevent cyber-attacks?				
9	Do you have anti-virus/anti-malware software protection?				
9(a)	If yes, when were they last updated?				
9(b)	If yes, how often are they run?				
10	Do you encrypt consumer personal information when transmitting it electronically (including by e-mail)?				

MASSACHUSETTS DIVISION OF BANKS
NON-DEPOSITORY INSTITUTION SUPERVISION
INFORMATION TECHNOLOGY OFFICER'S QUESTIONNAIRE

Question #	QUESTION	YES	NO	N/A	RESPONSE/COMMENTS
11	Can consumers conduct transactions, upload documents or manage accounts online? If yes, please describe.				
12	Do you have a written wire transfer policy in effect? If yes, please provide a copy of your policy.				
13	Do you employ access controls on consumer personal information systems?				
14	Do any third parties have access to your systems, including but not limited to, your organization's critical information and/or consumer non-public personal information?				
15	Do your employees have remote access? If so, please describe.				
16	Do you have an employee IT security awareness and training program?				
17	Have you changed operating systems or service providers since the previous examination? If yes, please describe.				
18	Are you planning to deploy any new operating systems, software, and/or engage any new service providers within the next 12 months? If yes, please describe.				
19	How do you dispose of confidential information, including paper and electronic records and equipment?				
20	Have you experienced any material incidents (internal or external) affecting your company's operations and/or your company's consumer personal information since the date of the last examination (or date of licensure, if first examination)?				
20(a)	If yes, please provide a description of the incident and what steps were taken to resolve the incident and notify consumers, if necessary.				
21	Does your company have a Disaster Recovery and Business Continuity Plan? If yes, please provide a copy of your plan.				
22	Do you maintain offsite backups of critical information? If yes, please provide details.				
23	How do you keep up to date with developing cybersecurity risks?				
24	Do you have a process in place to detect IT breaches?				
25	Do you conduct internal and/or external IT audits? If yes, how often are such audits conducted? Please provide a copy of your last audit report.				

ADDITIONAL COMMENTS OR INFORMATION

INFORMATION TECHNOLOGY OFFICER'S QUESTIONNAIRE

CERTIFICATION

I _____ **of the** _____
(Officer's Name/Title) **(Licensee Corporate Name)**

Of _____
(City and State)

Do hereby certify under the pains and penalties of perjury that the foregoing statements are true and correct to the best of my knowledge and belief.

This _____ **day of** _____ **20** _____**.**

_____ _____
(Signature) **(Date)**

This is an official document signed under the penalties of perjury