Attachment A
Documentation

Required Document	Security Handbook Chapter	Requirement	Additional Verifications
Access Procedures For DMH Applications	Chapter 4, Section II.D.	Access procedures are to be developed by DMH Access Coordinators. They need to describe who at DMH can be given access to the DMH Application, the level of access they can be given, and how such access will be approved and created	• Copies of each procedure are to be given to the DMH ISO • The procedures also need to be made available to DMH Supervisors of the DMH Workforce Members who will need to access such Applications
Auditing of Access	Chapter 8, Section IV, B.	To the extent possible, routine audit procedures and implementation documentation will be developed to determine appropriateness of user access based on applicable access table and/or procedures	
Auditing of Application Owners and Access Coordinators	Chapter 8, Section V.	Reports of all findings from routine audit of Application Owners and Access Coordinators	

Required Document	Security Handbook Chapter	Requirement	Additional Verifications
Business Continuity and Disaster Recovery Plan	Chapter 9, Section III. A. and D.	The Director of Emergency Management shall oversee the completion, revision, implementation and testing of a DMH wide Business Continuity and Disaster Recovery Plan. The Plan must address emergencies or disasters that could cause hardware, software or networks to become critically dysfunctional or cease to function Copies of the Plan are to be kept by the DMH ISO and by the DMH Director of Emergency Management. Workforce Members will have access to the Business Continuity and Disaster Recovery Plan and all Specific Plans as is necessary to ensure their proper implementation	The required contents of the Plan as well as time frame for developing it are set forth in Ch. 9, Section III
Computer Training Rooms	Chapter 6, Section IV, A. 6.	The DMH Learning and Development Office must maintain centrally a current list of all computer training rooms located in DMH Locations	Learning and Development needs to know how access to each room can be gained (e.g., who maintains the keys, etc.)
EPHI Systems and Databases	Chapter 3, Section II.	An Application Owner must register their EPHI System/Database with the DMH ISO The registration must be updated if there is a major change	• The EPHI System/Data-base Registration Form must be used • DMH ISO to maintain a current inventory of all DMH EPHI Systems/Data-bases

Required Document	**Security Handbook Chapter**	**Requirement**	**Additional Verifications**
Exit Checklist	Chapter 4, Section III. B.	DMH Supervisors will use the DMH Exit Checklist at the end of Chapter 4 to ensure the collection of all equipment and will submit all forms in a timely manner	
Identification Badges	Chapter 6, Section V.	Are to be worn by all DMH Workforce Members and visitors when at a DMH Location	The Handbook requires specific information to be included on the badges
Information Security Incident Reporting System	Chapter 2, Section III. D.	Incidents are to be logged into the DMH incident reporting system, currently the DMH RL6 Reporting System.	
Maintenance and Repair Records for Physical Site Security	Chapter 6, Section VI.	Each DMH Location must maintain documentation of all repairs and alterations made to the physical security components of the Location	The Handbook requires that specific information be captured in the documentation
Non-DMH Workforce Members Access to Commonwealth Network or to a DMH Application – Contract Required	Chapter 4, Section VI.	There must be a contract or MOU that contains very specific language	• Verify contents of contract/MOU • Verify that there is contract monitoring activity
Policies and Procedures	Chapter 1, Section IV.	A copy shall be retained for a minimum of six (6) years from the date the applicable policy or procedure was last in effect	

Required Document	**Security Handbook Chapter**	**Requirement**	**Additional Verifications**
Sanctions	Chapter 1, Section VI.	A report of all security related sanctions is to be maintained by the Human Resource Office for DMH Workforce Members Human Resources must make the information available to the DMH ISO on their request If sanction is against a non-DMH employee, the applicable DMH Supervisor is to notify the DMH ISO immediately	
Security Plan	Chapter 6, Section II.	Each Person in Charge is responsible for developing, implementing and documenting a Security Plan for their Location that addresses how Information Resources at their Location will be protected from unauthorized access, theft, loss, and environmental hazards Each Person in Charge is to retain a copy of their Plan in accordance with the Massachusetts Statewide Records Retention Schedule published by the Secretary of State's Office; provided, however, that a Security Plan must be maintained for a minimum of six (6) years from its last effective date	• The Handbook sets forth specific content requirements for the Plans, including, without limitation, an Access Card/Key Control Plan and Maintenance Records • The Plans are to be reviewed annually • Copies are to be given to DMH ISO

Required Document	**Security Handbook Chapter**	**Requirement**	**Additional Verifications**
System Specific Business Continuity and Disaster Recovery Plans	Chapter 9, Section III.C.and D.	Every Application Owner of an IT System or Database that is identified as supporting an essential DMH service or function is responsible for developing and implementing a contingency and disaster recovery plan for their System or Database To the extent possible, Access Coordinators are to develop similar Plans for DMH Applications	• Contents for the plans as well as time frame for developing them are set forth in Ch 9, Sec III.C • Plans must be approved by the DMH ISO and the ACIO
Training and Participation	Chapter 1, Section V.	Contents of all security training courses must be maintained by the DMH ISO Record of attendance of all trainings shall be kept in the EOHHS Learning Management System, currently MassAchieve	
Updates	Chapter 1, Section V.B.	DMH ISO to publish Security Alerts, periodically, as needed EOTSS and EHS IT may publish notices periodically, as needed	DMH ISO to retain copies of all Alerts sand Notices for minimum of 6 years from release date
Visitor Logs	Chapter 6, Section V.B.	DMH Locations are to maintain Visitor Logs for all visitors accessing Restricted Areas	Specific information is to be captured in the logs