16.1 PURPOSE:

16.1.1 The purpose of this document is to define the security procedures for the operation of the CODIS computer network and to meet the security requirements for participation in the National DNA Index System.

16.2 RESPONSIBILITY:

16.2.1 DNA Section Personnel and CODIS IT Personnel.

16.3 PERSONNEL SECURITY

16.3.1 Only approved CODIS users shall have access to the CODIS network hardware and CODIS software.

16.3.1.1 The CODIS State Administrator shall approve and add all CODIS users to the CODIS network and CODIS software. The CODIS State Administrator shall ensure that required documents including properly completed fingerprint cards for each proposed User are forwarded to the NDIS CODIS unit in accordance with the NDIS Operational Procedures Manual.

16.3.1.2 CODIS Users (DNA Analysts): The level of access of any CODIS User who is a DNA analyst to the CODIS software (read, add, modify, of delete DNA records) will be regulated by the CODIS State Administrator. DNA analysts will only have access to CODIS client devices. Client devices are defined as any computer (laptop, desktop, personal computer, workstation, etc.) running CODIS software with connectivity to the CODIS server.

16.3.1.3 System Administrators: The CODIS State Administrator, the Alternate State Administrator as well as Information Technology (IT) Personnel assigned to the DESPP who satisfy all requirements for a CODIS IT user in accordance with the NDIS Operational Procedures Manual may serve as System Administrators. Systems Administrators will have login access to the server and the client devices on which CODIS has been installed for operation and software maintenance purposes. System Administrators will not have access to the CODIS software. A CODIS IT User is not authorized to add, modify or delete DNA records from CODIS.

CODIS IT personnel shall reference the CODIS Information Technology guide that documents relevant information regarding the deployment, configuration and administration of the CODIS applications and environment.

In the event IT personnel not fully vetted to be a CODIS IT user require access to a computer or device with the CODIS software installed, this access shall be permitted only under the direct and constant supervision of the CODIS Administrator or an approved CODIS user.

16.3.1.4 CODIS SEN User: Laboratory personnel who may be granted access to the CJIS SEN (Criminal Justice Information Services Shared Enterprise Network). A CODIS SEN User is not authorized to add, modify or delete DNA records from CODIS.

16.4 CODIS ACCESS and PASSWORDS

16.4.1 Each CODIS user shall have an individual user account and password and must use these credentials each time they authenticate themselves to the system. CODIS access shall be configured to restrict each user to the least privileges required to perform authorized tasks. Each CODIS user shall use only his/her username and password to logon to the network. CODIS users are not permitted to use shared usernames and/or passwords.

16.4.2 The network privileges for each user shall be established and set by the CODIS State Administrator.

16.4.3 CODIS users will not be allowed to concurrently log onto more than one computer on the CODIS network at a time. The CODIS State Administrator and CODIS IT personnel may concurrently log onto more than one CODIS network computer at the same time, provided that any computer (s) not directly in use are locked and require a password for use.

16.4.4 All CODIS passwords shall expire after 90 days. Passwords shall include a minimum of 14 characters and shall contain three of the following character groups:

- Uppercase
- Lowercase
- Numeric
- Symbol

Passwords will not be one of the last 24 previously used passwords, changed within one day nor contain the user's account name or full name.

16.4.5 The CODIS server and all client devices shall be set to lock the screen after ten minutes of non-use and require the CODIS user's password to unlock the screen. All CODIS Users will be trained to lock or logoff of all CODIS computers prior to leaving the area in which the CODIS computer is located.

16.4.6 For CODIS Users who also perform administrative functions, two (2) user IDs shall be created: one (1) for normal CODIS user activities and one (1) elevated account for performing system administrative duties.

16.5 PHYSICAL SECURITY REQUIREMENTS

16.5.1 Physical security is defined as having controlled access to the laboratory and/or laboratory assets. The CT-DSS shall be responsible for providing adequate physical security for the CODIS server and client devices against any unauthorized access to the computer equipment or any stored data. No wireless servers or routers are allowed to be connected to any CODIS hardware.

16.5.2 The CODIS server and terminals shall be housed in access controlled portions of the laboratory. The server shall be housed in the server room of the laboratory. The server room has access limited to laboratory senior staff, laboratory IT personnel, the CODIS State Administrator, and the CODIS Alternate State Administrator.

16.5.3 The CODIS State Administrator and the CODIS Alternate State Administrator shall have keyed access to the laboratory's server room.

16.5.4 Backup copies of the CODIS data shall be stored in both the on-site and off-site locations in a lockable container.

16.6 CODIS COMPUTER SOFTWARE AND DATA SECURITY

16.6.1 CODIS software enhancements will be made available to the Laboratory via the secure CODIS intranet site or by digital media. CODIS software enhancements shall be downloaded from the CODIS secure intranet site and/or installed on each CODIS computer in accordance with NDIS supplied instructions in a timely manner.

16.6.2 The DSS will be responsible for ensuring any Commercial Off the Shelf (COTS) software, such as Microsoft Office and Adobe, installed on the server and/or workstations are properly maintained and updated when necessary.

16.6.3 The CT DSS subscribes to the automated software update service (WSUS) provided by the FBI. The State Administrator or Alternate Administrator will log in using their elevated account every 2 weeks to see if there are updates available to apply to the server and/or client devices. In the event NDIS sends notification regarding a WSUS update, the update will be completed by the specified deadline.

16.6.4 CODIS DNA profile data shall be backed up on a daily basis (weekdays) to an external backup source. All backup files shall be encrypted in compliance with the NDIS Security Requirements. The CT-DSS uses Backup Exec which has been modified to support CODIS Full Backup jobs to be encrypted. Once a month, the external backup media that contains the most current copy of the CODIS DNA profile data shall be stored at an off-site location.

16.6.4.1 The electronic backup media that contains the CODIS DNA profile data to be stored at the laboratory shall be kept in the server room in a lockable container. The location of key for the lockable container shall be known to the laboratory's IT personnel, the CODIS State Administrator, the CODIS Alternate State Administrator, and the Assistant Director of Forensic Biology/DNA. An additional key for the lockable container shall be stored with Division Administration.

16.6.4.2 The electronic backup media with the CODIS DNA profile data that is stored off-site shall be kept in the server room of the CT Department of Emergency Services and Public Protection Headquarters (DESPP HQ) building located in Middletown, CT. The DESPP HQ server room is a secure access controlled facility. The data shall be kept in a lockable container. The location of the key for the lockable container shall be known to the laboratory's IT personnel, the CODIS State Administrator, the CODIS Alternate State Administrator and the Assistant Director of Forensic Biology/DNA. An additional copy of the key shall be stored with Division Administration.

16.6.4.3 The integrity of the backup files will be verified on a quarterly basis using the Hash Compare program. Hash Compare is a hash based comparison tool that performs a data integrity evaluation to detect problems that may occur due to faulty storage media, as well as errors that could occur in either the transmission or writing of data. Hash Compare verifies that the CODIS database backup file matches the file that has been transferred to the external electronic media.

16.6.4.3.1 The Hash Compare program is launched using an elevated account on the CODIS server at the following location: D:/CODIS/CODIS70SP7/Migration/HashCompare
The newly created versions of following two .bak files will be located and selected for comparison:

1) C:\HASH\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup\CODIS\CODIS_backup_20xx_xx_xx….bak
2) D:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup\CODIS\CODIS_backup_20xx_xx_xx….bak

Note: 20xx_xx_xx = date files were created

16.6.4.3.2 Confirm/Select the Hash Type as MD5 and click the "Compare Files" button. When the comparison is completed observe the Result of Comparison. If the files are identical, export the report to the Hash Compare Results file and print the report. If the files are not identical, report this information to the CODIS Administrator who will contact CODIS HelpDesk and inform the Technical Leader and Assistant Director.

16.6.5 The appropriate anti-virus definitions will be downloaded from the CODIS website on the CJIS SEN and run on the CODIS server and each CODIS workstation in a timely manner. This action will occur no less frequently than once a week.

16.6.5.1 The CODIS IT User, the CODIS State Administrator or the CODIS Alternate State Administrator will be responsible for downloading and running the anti-virus definitions on the server

16.6.5.2 The CODIS Administrator or the Alternate Administrator will be responsible for downloading and running the anti-virus definitions on the CODIS workstations.

16.6.6 The following actions taken on the server and/or client devices will be documented on the CODIS Maintenance Log by listing the details of the action taken, the date of action and the initials of the individual performing the action.

- Installation of CODIS software enhancements (e.g. Service Packs, Hotfixes)
- Installation/updates of COTS software.
- Biweekly check of software update service (WSUS).
- Monthly backup of CODIS data and storage of media off-site.
- Weekly antivirus downloads.
- Shutdown/reboots of the server/network.
- Any upgrade/maintenance/repair/replacement of any hardware on the network.
- Quarterly backup data integrity checks using Hash Compare.

This log will be periodically (at least once every 60 days) checked by the CODIS State Administer. This check will be documented in the CODIS Maintenance Log.

16.7 CODIS DISASTER RECOVERY PLAN

16.7.1 Server repair/failure. In the event of the partial/total failure of the CODIS server, an emergency request for repair/replacement shall be made to the Department's purchasing office. The Department has sufficient emergency equipment repair/replacement funds, such that the repair/purchase of a new server would be possible.

16.7.2 Damage to the laboratory. In the event of damage to the portion of the laboratory housing the CODIS server, the server will be moved to an undamaged portion of the laboratory and the CJIS-SEN connection rerouted. In the event that a disaster has made the entire laboratory unoccupiable, the CODIS server and CJIS-SEN router will be moved to an alternate secure Department building with a preexisting CJIS-SEN connection. NDIS and CJIS-SEN will be contacted and a request for an emergency connection will be made.

16.8 CODIS NETWORK SECURITY

16.8.1 The CODIS software shall only be installed on computers that do not have access to the Internet. No computer with installed CODIS software shall be connected to any network with Internet access.