4.0 – SECURITY

In order to maintain the integrity of the CODIS network within TBI both at the SDIS and LDIS levels, several layers of security measures exist.

4.1 Physical Measures - Nashville

4.1.1 The building must have intrusion and fire alarm systems in place.

4.1.2 The CJIS-WAN equipment provided by the FBI is located in a controlled access TBI computer hub area.

4.1.3 CODIS reports and logs will be kept in secured areas.

4.1.4 Computers with access to CODIS software will be located in areas that are only accessible by TBI security badges. Unsupervised access is granted to the Forensic Biology supervisor(s), CODIS supervisor(s), CODIS administrator(s), DNA analysts, and CODIS technicians as well as members of the TBI Management staff, which includes the TBI Assistant Director - Forensic Services Division, Regional Administrator(s), Forensic Manager(s), Forensic IT Manager, DNA Technical Leader and/or Building Emergency Response Team members.

4.1.5 Repair personnel working within the Forensic Biology and CODIS unit(s) must wear visitor security badges and be escorted while in the laboratory.

4.1.6 Repair personnel are not allowed to remove the hard drives or security implementation from computers and take them from the building. If hard drives must be replaced, they will first be reformatted by the FBI, CODIS administrator(s), or their designee and destroy the programs and data stored on them.

4.1.7 Physical arrestee and convicted offender samples will be housed in a secure climate-controlled storage area with limited access. Access should be limited to members of the CODIS unit in Nashville plus a limited number of TBI Management. Access logs for all secured areas are maintained by the TBI Uniformed Officers.

4.2 Physical Measures – Knoxville and Jackson

4.2.1 The building must have intrusion and fire alarm systems in place.

4.2.2 Computers with access to the CODIS software will be located in areas that are only accessible by TBI security badges and/or personalized pin numbers. Unsupervised access is granted to the Forensic Biology supervisor(s), CODIS supervisor(s), CODIS administrator(s), DNA analysts, and CODIS technicians as well as members of the TBI Management staff, which includes the TBI Assistant Director - Forensic Services Division, Regional Administrator(s), Forensic Manager(s), Forensic IT Manager, DNA Technical Leader and/or Building Emergency Response Team members.

4.2.3 All CODIS software and equipment is maintained at TBI headquarters in Nashville.

4.2.4 Analysts and administrators with access to CODIS software must lock computers when not in use or when they are away from their desks.

4.3 Computer Measures

4.3.1 The CODIS administrator at each local lab shall be responsible for ensuring that only approved CODIS users have access to CODIS. Only the CODIS administrators (including administrators in Jackson and Knoxville) and forensic scientists within the CODIS unit shall have full privileges to all CODIS functions. Casework DNA analysts are granted limited working privileges within CODIS. Individuals granted limited access to CODIS, such as Information Technology (IT) personnel within TBI are classified as Non-Host Users and as such are afforded no working privileges to CODIS functions. IT personnel have Non-Host User access to CODIS for software maintenance purposes only. The CODIS administrator is responsible for the initiation and termination of privileges to the CODIS network for any individual.

4.3.2 All TBI CODIS equipment and logs will be maintained according the NDIS Security Policy and TBI policy.

4.3.3 No software is to be loaded onto CODIS computers without prior approval from the system administrator. All software will be scanned for viruses before being loaded onto CODIS computers. Data and software will not be downloaded from third party systems without previously being searched for viruses. Virus protection definitions will be updated monthly.

4.3.4 Backup of data on CODIS servers should be performed weekly. A monthly full backup of data on CODIS servers will be performed and will

be stored off-site at another regional facility. This backup data will be utilized should the laboratory or computer system become disabled.

4.3.5 The CODIS administrator is to be notified immediately if computer crime is suspected. This may include but is not limited to: unauthorized entry into a computer system, loading of unauthorized software, and misuse of the computers or software.

4.3.6 Forensic Biology unit employees will log out of the CODIS software when leaving their personal computer area. Computers should be locked when not in use.

4.3.7 Computers with access to the CODIS software will comply with all NDIS security measures, including but not limited to implementing a mandatory time-out function after a period of inactivity.

4.4 Personnel Measures - Passwords

4.4.1 Passwords shall be at least 12 characters and contain three of the four following components: English uppercase characters (A through Z), English lowercase characters (a through z), base ten digits (0 through 9), or non-alphabetical characters (e.g. $, #, %, *). The password should be complex and difficult to guess. It is strongly advised that they not contain the user's name, children's names, etc.

4.4.2 Passwords will be changed at least once every 90 days. Display of passwords is prohibited. Users should not have passwords written down and placed in locations that can easily be found. Passwords shall not be disseminated over the phone, through the mail, or through other computer systems.

4.4.3 If an analyst believes password security has been breached, that analyst will immediately change the password and inform the system administrator in writing within 24 hours of discovery. If a password is revealed to another individual, that password must be changed as soon as possible.

4.5 Access to Data Information

Access to personal identifying information in CODIS is permitted via request from sample collection sites, law enforcement, or criminal justice agencies. It is suggested that all requests be in writing. Limited information will be given to collection sites (i.e.,

upon request a collection site may be informed if we have samples from certain individuals). Only a CODIS administrator with access to database information may release this information to a law enforcement agency or to a member of the CODIS or Forensic Biology unit(s); members of those units may disseminate the information to law enforcement agencies. CODIS technicians may release information with approval from a CODIS administrator. Requests for CODIS information from outside agencies (non-law enforcement agencies and non-criminal justice agencies) or private individuals must be submitted in writing and reviewed by the TBI legal unit. Response to the request may be released only by a CODIS administrator, the TBI Assistant Director - Forensic Services Division, Regional Administrator, or Forensic Scientist Manager.

4.6 Access to DNA Samples

4.6.1 Requests from an agency or individual for a portion of a sample from an offender or arrestee will not be granted unless it is the only known sample from a now deceased individual. In order to process such a request, the following procedure must be followed.

4.6.1.1 The agency or individual must first submit a written request (on letterhead if an agency or legal agency) containing the full name, date of birth (DOB) and social security number (SSN) of the offender or arrestee.

4.6.1.2 A CODIS administrator will notify the requestor in writing (via letter or email) if that individual is in one of the databases and inform the requestor that TBI cannot verify the identity of the individual since no chain of custody exists.

4.6.2 If the TBI has a sufficient amount of sample from the requested individual, the following items are required to obtain a portion of the samples and this list must be sent in writing to the requestor.

4.6.2.1 Proof that the individual is deceased (i.e. copy of a death certificate).

4.6.2.2 A court order signed by a judge stating the reason the sample is being requested. A legal matter, such as a paternity case, is the only acceptable reason. The court order must contain the full name, date of birth (DOB), and social security number (SSN) or state ID number (SID) of the deceased. The letterhead or court order must contain the explicit reason for the use of the DNA sample.

4.6.2.3 Instructions for where the sample needs to be sent must be included in the letterhead. If the TBI is to send it directly to the lab performing the analysis, a statement will be needed either in the court order or in writing on letterhead that TBI is not responsible for any payment for the analysis.

4.7 Access to DNA Profiles

4.7.1 Submitting agencies may request a copy of a casework DNA profile for use in a John Doe Warrant. The request must be made in writing on agency letterhead that contains the TBI laboratory number of the case where the DNA profile was obtained, the signature of the agency investigator as well as the District Attorney, and the following statement, “If a hit develops from the DNA profile listed in the John Doe Warrant, a known sample (blood or buccal) will be submitted immediately to the TBI laboratory for confirmation.”

4.7.2 DNA profiles in CODIS will not be used as standards for comparison in casework.

4.8 Contingency Plan

4.8.1 In the event that a CODIS server is down for a short period of time (e.g. power failure or computer issue), the CODIS Help Desk must be informed.

4.8.2 In the event that a CODIS server is non-functioning for an extended period of time, the CODIS administrator may use the computer backups of the server in order to maintain day-to-day operations.

4.9 Server Maintenance and Changes within the CODIS Software

4.9.1 Server maintenance is performed during non-working hours by TBI IT personnel who are approved CODIS IT users. After CODIS servers undergo maintenance, a performance check via a checklist will be performed by a CODIS administrator (a CODIS user with administrative rights within the CODIS software). The performance check for SDIS includes the completion of an upload to NDIS and completion of the daily searches at SDIS. Performance checks at LDIS will include a successful upload to SDIS.

4.9.2 Any changes made to the CODIS software in the “Options” menu related to specimen categories, loci, autosearches, or other applicable sections must have a performance check done. A CODIS administrator shall write

up a plan for testing the new change and it must be documented and approved by the state CODIS administrator. Each plan will be specific to the change made and shall test the core components of that specific option function.

4.10 Paperless Processes in CODIS

4.10.1 The CODIS unit in Nashville utilizes digital processes to collect, store, and report technical and administrative data without having to use traditional paper-based records. All data created for placement in laboratory casefiles will be retained digitally in a secure environment within the internal TBI computer network. Specific details about report construction and requirements can be found in the reporting sections of the TBI CODIS Manual.

4.10.2 Technical and administrative documents created for CODIS hits and CODIS No Match reports for TBI cases should be retained in LIMS. The paperwork shall be retained in the TBI case file per TBI policy.