In order to protect confidential and sensitive information from those unauthorized to have access to it, the SBI Molecular Genetics Section will follow the following security procedures:

1 USE OF PASSWORDS

1.1 Each computer user will use passwords to protect programs and data.

1.2 Passwords selected will be ones that are difficult to guess.

1.3 Display of passwords is prohibited. Users should not have passwords written down and placed in locations that can easily be found.

1.4 Passwords are not to be given out over the phone, through the mail, or through other computer systems.

1.5 The CODIS software provides password protection for that software. CODIS authorized users are not to reveal their passwords to anyone else. Each CODIS user will have a unique identifier.

2 PHYSICAL SECURITY MEASURES

2.1 All Section computers are located behind the section entry door. The building has an intrusion and fire alarm system and the building is secured after hours by the presence of a Capital Police officer. Keys to Section facilities and individual rooms in these facilities are tightly controlled and restricted.

2.2 If computer assistance is needed, the appropriate Personnel should be notified. Personnel repairing computers that are not authorized to have CODIS access shall not be allowed to directly access the CODIS system and analysts should not be logged into CODIS when repairs are underway.

2.3 All other repair personnel working on Section computers are to be escorted at all times while in the Section. Repairmen will not be allowed to remove hard disk drives or security dongles from Section computers and take them from the building. If hard disk drives have to be replaced, they will first be exposed to strong magnets or undergo low level formats so as to destroy the programs and data stored on them.

2.4 The CODIS file server is particularly sensitive and the room in which it is located will be locked. The only individuals that will have access to the file server room are the Section SAC, the CODIS System Administrator, and his assistants.

3 COMPUTER SECURITY MEASURES

3.1 NC Government policy for use of computers will be followed.

3.2 CODIS computers are to be used for SBI business only.

3.3 Games other than those supplied with the Windows program are not to be stored or used on Section computers.

3.4 The CODIS Administrator will put stop privileges on the CODIS software for any employee who leaves the SBI.

3.5 Every Section employee is to immediately notify the SAC if computer crime is suspected. This may include but is not limited to unauthorized entry into a computer system, misuse of Bureau computers and software, etc.

3.6 No software is to be loaded onto Section computers by the users. The only persons authorized to load software on Section computers are the Special Agent In Charge (SAC), the CODIS System Administrator, or other authorized personnel.

3.7 All software will be searched for viruses by appropriate parties before being loaded onto Section computers.

3.8 Data and software will not be downloaded from third party systems.

3.9 Users must sign off when leaving the CODIS network.

3.10 All users of CODIS software must understand that this is a stand-alone system. CODIS computers will not be connected to any other network (except CJIS-WAN and DCI Security personnel thru our firewall computer).

3.11 All software in use in the Section will be properly licensed.

3.12 Section employees will not browse through the disk drives of other analysts' computers. No Section employee is to utilize someone else's computer without the express consent of the assigned user or the SAC.

3.13 All personal computers and file servers will be connected to UPS systems.

3.14 A strict prohibition is in place on reading of E-Mail of others.

4 CONFIDENTIAL INFORMATION HANDLING PROCEDURES

4.1 All case related data and information generated in the course of business considered CONFIDENTIAL and covered by the same NC General Statutes that apply to all other SBI files and records.

4.2 Criminal penalties can be attached in the event genetic information is misused as per NC General Statute §15A-266.

4.3 Casework files, reports and data as well as individual identifying information on victims, suspects, and convicted offenders are of particular concern. Casework files are protected by procedures found in the Crime Laboratory Procedures Manual. Offender files are covered in the DNA Database Unit Procedures Manual. All computer generated printouts of confidential information that are no longer needed MUST be destroyed by shredding prior to being placed into the trash.

4.4 CODIS data files and software are to be transferred to appropriate parties (e.g. SAIC) via Registered Mail or via downloading through the CODIS environment.

4.5 All requests for CODIS files, genetic information, or information concerning identifying information found in CODIS from non-CODIS laboratories will be handled only by the CODIS System Administrator, his assistant, or the SAC.

4.6 No one will give identifying information accompanied by a genetic profile to anyone outside the CODIS system unless authorized to do so and unless they are sure that the person given this information is authorized to have this information.

5 TRAINING

5.1 All Section employees are to receive training in computer security measures. This

training will consist of individuals reading this document, review of this document by the SAC with all employees, and each employee will sign and date the attached form stating that they have read and understand this document and the date of training.

5.2 Members of the IT PC Group will be provided a copy of this security document

6 SANCTIONS

6.1 Anyone revealing the genetic profile of an individual in the DNA Database to unauthorized personnel may be subject to criminal penalties as per NC General Statutes § 15A-266.

6.2 Non-compliance with established security policies, standards, or practices are grounds for disciplinary action.

RECEIPT AND UNDERSTANDING OF THE NORTH CAROLINA STATE BUREAU OF INVESTIGATION MOLECULAR GENETICS SECTION COMPUTER SECURITY PROCEDURES

I, _____ received a personal copy of the above listed document on _____. I have read and understand the information present in this document and have had an opportunity to ask questions about the contents of this document. At the time I received this document, its contents were discussed in a meeting and the intent was covered by the SAC.