



State of North Carolina
Department of Public Safety
POLICIES & PROCEDURES

INFORMATION TECHNOLOGY

Division: ADMINISTRATION
Chapter: INFORMATION
TECHNOLOGY
Policy: COMPUTER
RELATED
INVESTIGATION
Issue Date: AUGUST 13, 2013
Revised:

I. PURPOSE

To assist management in conducting internal reviews of information systems as the result of suspected or actual policy violations.

II. SCOPE

This policy applies to all employees, including permanent, contractual, temporary, and consultant employees who work for the Department of Public Safety and use the Department of Public Safety computing and networking resources. All users are expected to become familiar and comply with the guidance provided herein. Questions regarding this policy should be directed to the Department of Public Safety's Information Security Office.

Statutory and/or Regulatory Authority: State Information Security Manual; G.S. §147-33.110, Statewide security standards; G.S. §147-33.113, State agency cooperation.

III. POLICY

Preliminary Investigations of Employees

In cases where there is a suspected policy violation or misuse of computer resources, a DPS manager may request a preliminary review of the system involved. The preliminary review will consist of a search by MIS staff for any evidence to support or alleviate management's suspicions. MIS staff will discuss the results of the preliminary review with the requesting manager. Confirmation of a policy violation may, at the request of the manager, lead to a Full Investigation (see below).

Full Investigations of Employees

A full investigation can only be initiated through an appropriate DPS manager by contacting the DPS Information Security Office. The Information Security Office will determine who should perform the investigation. The investigator may then examine any computer files containing documentation or other evidence which may be relevant to the investigation. This may include, but is not limited to letters, memoranda, expense records, telephone records, time records and e-mail. Care should be taken to comply with the department's personnel policies and applicable

laws and policies governing interception of electronic messages and privacy/confidentiality.

- A. Confidentiality. All information gathered during the investigation shall be treated as confidential and disclosed only on a need-to-know basis.

REFERENCE: Article 7 of G.S. §126, The Privacy of State Employee Personnel Records; Article 29, Records and Social Reports of Cases of Abuse, Neglect, and Dependency; Article 30, Juvenile Records and Social Reports of Delinquency and Undisciplined Cases; Article 31, Disclosure of Juvenile Information; and G.S. §132-6.1(c), Electronic data-processing records.

- B. Investigation Records. Detailed written records of each step of the investigation should be maintained, including witness interviews, date and time of interview, and when the computer was examined. All such records should be maintained in confidential investigation files and a written Chain of Custody document should be maintained for all evidence collected. The Chain of Custody documentation is important and assures continuous accountability. Managers should remember that all investigative records may be subject to discovery should the investigation result in litigation and document the investigation accordingly.
- C. Computer Collection. The employee's computer may be collected directly by the Information Security Office and/or properly trained and assigned personnel and then properly packaged and transported to the Information Security Office. Personnel assigned to collect an employee's computer will ensure that proper procedures are followed for packaging, transporting and storing electronic evidence to avoid alteration, loss, physical damage or destruction of data.
1. If criminal charges are a likely outcome of the investigation, the SBI should handle the collection and examination directly.
 2. If the DPS manager has reason to believe that the employee may try to destroy evidence, then the collection should be done as quickly as possible.
 3. In non-criminal, personnel matters, it may be sufficient to investigate the computer after work hours and return it to the employee's workspace before the next business day.
- D. Computer Examination and Reporting. The Information Security Office and/or properly trained and assigned personnel should examine the computer using forensic software and record the following information:
1. Reason for examining the PC including who gave the authority for the investigation.

2. Date and time of collection.
 3. PC serial and model numbers.
 4. If the PC was powered on, what was on the screen.
 5. Printouts or other reports of suspicious files found by forensic software on the hard drive.
 6. Network files, backup tape data and other media (e.g. Flash memory cards, floppies, diskettes, CDs, USB drives, jump drives and other electronic devices and peripheral evidence) relating to the case.
- E. Closure of Investigation. The Information Security Office will be responsible for the close-out of the investigation.
1. A written report will be generated.
 2. The Information Security Office will review all findings and distribute the report to the appropriate contacts. This is important because State Statutes require the Information Security Office to report certain computer security incidents. Privacy/Confidentiality laws and policies shall be adhered to in this exchange of information.
 3. If potential criminal findings are identified, the Information Security Office will provide a copy of the report to outside law enforcement such as the SBI or FBI.
 4. The Prison Rape Elimination Act (PREA) Office shall be immediately notified of any allegation or suspicion of inmate or juvenile resident sexual abuse or sexual harassment; as well as any allegation/suspicion of undue familiarity.
 5. The investigative report and, if any, corresponding data will be maintained and secured by the Information Security Office.
 6. There is a 7-year retention period for investigative reports.

Special Provision for Computer Investigations

In cases where a DPS division has staff trained to perform full computer investigations, the division shall prepare an annual written blanket request to conduct computer investigations for their division. The request should be submitted to the DPS Information Security Office and should include the computer investigation procedures and processes that are to be used by the requesting division, staff qualifications, training received, certifications, and any other pertinent information. Divisions authorized to perform their own investigations shall notify the DPS

Information Security Office prior to performing any computer investigation and provide the results of the investigation to the DPS Information Security Office. Unless requested, specific details surrounding these investigations can be excluded from the correspondence to the DPS Information Security Office.