	Administrative General Order	4.02 Information Technology	PAGE 1 OF 3
	SUBJECT **Virginia Beach Police Department General Order** Chapter 4 - Reporting and Fiscal Management		EFFECTIVE DATE **04/06/2011** ORIGINATOR/REVIEW Support Manager
	DISTRIBUTION ALL	**CALEA: 11.4.4, 41.3.7 A, B, 82.1.1 A, 82.1.6**	
BY THE AUTHORITY OF THE CHIEF OF POLICE: James A Cervera			

Purpose

The purpose of this general order is to describe the policy regarding computer access and use, system integrity, application audits, and system backups.

Policy

It is the policy of the Virginia Beach Police Department that all members (including employees, volunteers, temporary contractual) abide by City Administrative Directives 2.04 (Network Acceptable Use), 2.06 (Information Technology Infrastructure and Asset Management), 2.09 (Information Security and Privacy Office Charter), and the procedures set forth herein when using computers, databases, and other automated information.

The Department of Communications and Information Technology (ComIT) in conjunction with the Police Support Division work together to provide electronic data processing, Internet/Intranet systems, and other information technology resources to members of the department and to the public.

Department computers, including mobile data terminals, are to be used only for the official business of the City of Virginia Beach. This includes E-mail, Internet/Intranet access and access to any and all city information systems.

System Security and Access (CALEA 82.1.1 A, 82.1.6 C)

The protection of police data files is essential to the public trust. All files, including email, stored on a City computer are City property. The data maintained in these files are official records and shall be used for law enforcement or official City business purposes only and not for an individual's commercial use or profit, or for secondary employment not associated with the City. Data security is the responsibility of everyone accessing the data. The Chief of Police or designee may suspend or rescind access to police files or folders for security reasons.

There are several levels of information security protecting police records, including physical security, network password security, and application password security. All automated records held by the Virginia Beach Police Department are physically secured in locked work areas where access is limited to authorized personnel only. Access to police files and folders is restricted to authorized members who have an approved job-related business need for the information.

Members of the department and other authorized individuals are assigned computer user identifications (user ID) and passwords to control access to the Records Management System and other computer resources. The user ID and passwords will remain confidential and shall not be shared with others in order to guard against unauthorized access and protect the integrity and confidentiality of the data. Members are required to lock or log-off the computer when it is left unattended.

All Police Department members are required to read and sign a Confidentiality Agreement (PD-7) prior to being granted access to police systems. Once signed, the original PD-7 is sent to the Chief's Office and a copy is maintained in the employee's Personnel File within their command. City employees from outside the Police Department (such as from the Sheriff's Office, Emergency Communications and Citizens Services Department, Probation and Parole, Fire Department) who access Police systems will sign a separate Confidentiality Agreement prepared by the Police Department unless that department has an internal Confidentiality Agreement acceptable to the Police Department.

Access to the Law Enforcement Information Exchange (LInX) and the Virginia Criminal Information Network/National Crime Information Center (VCIN/NCIC) are governed by separate agreements with the Virginia LInX Board of Directors and the Virginia State Police, respectively. A Memorandum of Agreement between the Police Department and Department of Communications and Information Technology (ComIT) sets forth standards of security consistent with federal and state laws and regulations, including the Federal Bureau of Investigation's Criminal Justice Information Systems Security Policy.

The City's Department of Communications and Information Technology (ComIT) is responsible for enabling and disabling access to the City's enterprise computer network and email and have procedures in place to regularly disable accounts for employees separating from City employment. If a Police Department employee is under criminal investigation, retires, resigns, is terminated, or leaves the agency for any reason, the Police Department's Systems Analyst or designee is responsible for immediately disabling their access to police applications such as the PISTOL™ records management system, LinX, VBPDnet, and COPPSnet (Community Oriented Probation and Parole Services Network) - Virginia Department of Corrections. The Police Systems Analyst or designee will also notify ComIT that the employee's access to the City's enterprise network and email should be immediately disabled if the employee was terminated or for other reasons as determined by the Chief of Police or his designee. All other systems accessed will be disabled via ComIT or ComIT notifying the responsible party, i.e. CADS, Supreme Court Case Management, Virginia Employment Commission (VEC), IPOAD, VCIN access via CADS (through mobile data terminals), GLink, OpenFox™ Messenger, etc.

ComIT charges a base fee to move computer equipment. Computer equipment relocated by the user requires notifying the Police Support Division System's Analyst, who maintains an inventory list of all computer locations. Workstations with access to Virginia Criminal Information Network (VCIN) shall not be moved without prior approval from the Police Department's VCIN Coordinator and written permission from the Virginia State Police. Internet access is prohibited on computers that have access to VCIN.

Members are required to submit a ComIT Network Access Request form to the ComIT Support Center (Help Desk) any time there are changes to their names, job title, phone/fax numbers, or assignment location.

System Audits (CALEA 82.1.6 D)

Members shall not make any unauthorized copies, creation, destruction, deletion, or alteration of city or department computer data, software, or hardware. This includes entering or modifying data or information that the person making such entry knows to be false.

All department computers are subject to audits at the discretion of the Chief of Police, his designee, or the City's Information Security or Privacy Officer. Information from emails, histories, logs, data files or programs that indicate a department computer has been used for purposes outside this policy will be directed to the member's chain of command for appropriate action. The Police Systems Analyst will conduct a documented annual audit to include, at a minimum, all user IDs and passwords for PISTOL™ and VCIN. Access violations may be tracked at the request of the Chief of Police or designee. The Police Systems Analyst will also conduct an annual security audit of the COPPSnet and LInX systems to comply with the external agency audit policies.

Introduction of Outside Computer Software (CALEA 11.4.4, 41.3.7 A, B)

Internal and external computer components or any software shall not be installed or modified in any way without approval of the Police Support Division or ComIT. Prior to authorized downloads or installs of any file including sound and video files and files attached to E-mail messages, software, or other materials from the Internet or other external sources, it shall be the member's responsibility to inspect for computer viruses using software provided by ComIT.

Backup and Storage Procedures (CALEA 82.1.6 A, B)

Computerized police records shall be stored on a secured network with data access via police-approved application**s** only. Police network server backups are performed on a regular basis by the Department of Communications and Information Technology. Backup procedures for files maintained on individual workstations are the responsibility of the member.