# OVERLAND PARK POLICE DEPARTMENT
# STANDARD OPERATING PROCEDURE

**NUMBER:** 3010
**TOPIC:** SPECIAL INVESTIGATIONS
**EFFECTIVE DATE:** 02/13/2017
**SUPERCEDES:** 03/07/2008

**SIGNATURE:** */s/ Frank Donchez* — **Chief of Police**; */s/ Simon Happer* — **Bureau Commander**



CALEA references: see below

## I. PURPOSE

The Overland Park Police Department places an emphasis on providing a safe environment by performing quality case and special investigations through identifying, apprehending and prosecuting suspected criminal offenders**.**

## II. PROCEDURE

A. RESPONSIBILITIES 43.1.1(A)(B)(C), 43.1.5

The Investigations Division will handle Special Investigations and will proactively but lawfully maintain an investigative capability to identify, apprehend and prosecute suspected Cyber-Crime, Drug, Vice. and Gang offenders. Special Investigations sergeants will review and assign reports, tips, and leads to detectives for follow up investigation. Detectives will complete reports or supplemental report(s) documenting their investigative follow up.

Special Investigations sergeants will maintain an electronic record of complaints received. Special Investigations personnel will provide support for case detectives through physical and electronic surveillance, case investigation, technical and analytical assistance. Additionally they will provide information and intelligence gathering capability in reference to ongoing criminal initiatives and enterprises; and, ensure records and reports relating to vice, narcotic, and organized crime investigations are securely filed and maintained separately from the central records system which are compliant with 28 C.F.R part 23.

Special Investigations will maintain a database of suspected and known criminals, to include specific information about the individuals' methods of committing crimes. They will maintain a record of information conveyed to and received from outside agencies. They will disseminate, directly or through the Crime Analysis Unit, information to all selected Members and other law enforcement agencies in a manner designed to effectively abate criminal activity and create proactive suspect apprehensions.

As a part of their responsibilities, detectives assigned to Special Investigations will need to conduct or participate in surveillance, undercover, decoy, and raid operations. Detectives will complete a *Police Department Operations Plan* and obtain approval from an Investigations Division supervisor prior to engaging in these activities.

## B. EQUIPMENT, AUTHORIZATION, AND CONTROL

The Special Investigations Sergeant is responsible for maintaining, issuing, and inventorying all equipment assigned to Special Investigations. This equipment includes but is not limited to any surveillance and undercover equipment.

## C. UNIT STRUCTURE 43.1.1(D)

The Investigations Division Commander oversees Special Investigations and is responsible for advising the Chief of Police regarding Special Investigation activities.

The designated Investigations Division Captain is responsible for Special Investigations. The Drug and Intelligence Unit detectives are supervised by the Special Investigations Sergeant. The Cyber-Crime, Vice, and Human Trafficking Unit detective(s) are directly supervised by the Special Victims Sergeant.

## D. CYBER-CRIME SECURITY & ACCESS

Cyber-Crime investigations are extremely sensitive in nature. All Cyber-Crimes detectives will be held strictly accountable for ensuring all computer evidence is properly collected and maintained. All Cyber-Crimes operations will be housed in a secured office setting controlled by assigned Cyber Crimes keys. Visitor access to the secured office will be restricted. Those with authorized access and issued Cyber-Crimes keys will be limited to the following:

- Chief of Police and Bureau Commanders
- Investigations Division Commander
- Investigations Division Captain(s)
- Special Investigations Sergeant(s)
- Cyber-Crime assigned Members.

## E. CYBER CRIME VISITOR RESTRICTIONS

Visitors authorized for temporary and restricted access include personnel with legitimate business purposes, and visitors approved by the Chief of Police or a Bureau Commander.

All visitors approved for temporary access will adhere to the established criteria for temporary access, and will be escorted by personnel approved for authorized-access status.

Requests to use an unfiltered computer, if considered legitimate and professional, will be submitted to the Special Victims supervisor for review and approval.

The Special Victims supervisor will assign the visitor to a cyber-crimes detective who will assist the visitor with their investigative needs. At no time will a visitor be left unattended in the cyber-crimes area.

## F. CITY & OPPD COMPUTER POLICIES

When accessing any non-covert network City computer in the Cyber Crime Office, personnel will always abide by City and OPPD policies related to computer use.

Authorized use of covert network computers during sensitive investigations will require deviation from City policies, rules and procedures; however, all follow-up by investigators and analysts will be legitimate, proper and professional.

All computers within the Cyber-Crimes office are subject to random audits. If during any sensitive investigation, investigators or analysts become involved in any inadvertent and unintentional viewing considered inappropriate per policies, rules, and procedures, the he/she will report such viewing to a Special Investigations supervisor. The investigator or analyst will note such in the *Cyber-Crimes Activity Log* by documenting the Supervisor notified, date & time, activity or work, site searched, and Case/Lead number.

## G. CYBER CRIME COMPUTER PRIVACY & SECURITY

Personnel will never have any expectation to nor right of privacy for any data files, software, or information stored on Unit computers. Members will not allow or assist Non-Unit Members to access any Cyber-Crimes office computers without supervisory approval as outlined herein.

Members will not release or share any personal identification codes, access codes, passwords, or Secure ID tokens with others. Members will not violate any software licensing agreements for purchased software or load or knowingly use any personal or unlicensed software.

Members will protect computers and software from theft, damage, destruction, misuse, unauthorized use, accidental or purposeful modification, unauthorized access or tampering. Members will log off or lock all computers when they plan to be away from the Office for an extended period of time.

Origin Date: 12/18/2007
Revision Date: 03/07/2008
Revision Date: 02/13/2017

CALEA references:
43.1.1(A)(B)(C)(D)
43.1.5