University of Chicago Police Department
GENERAL ORDER

	Effective Date February 20, 2018	***Number*** **GO 202**
Subject: **Supervision and Accountability and Computer Security**		
References: CALEA Standards: 11.3.1, 11.3.2, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 41.3.7, 53.1.1		
Reevaluation Date Annually		***No. Pages*** 3
Amends 30 JUN 2017 Version 19 AUG 2013 (O.D.P.)		*Rescinds:*
Approved By: Kenton W. Rainey, Chief of Police	Signature: Original signed document of file in Accreditation Office	

202.1 PURPOSE

The purpose of this order is to describe Department supervision and accountability.

202.2 AUTHORITY AND RESPONSIBILITY

An employee cannot be held responsible for the accomplishment of an order unless the authority necessary for its accomplishment has been given. Therefore, at every level in the Department:

A. Responsibility shall be accompanied by commensurate authority.

B. Each employee shall be accountable for the use of delegated authority.

C. Each employee is accountable to only one supervisor at any given time.

202.3 SUPERVISORY ACCOUNTABILITY

A. Supervisory personnel shall be accountable for the activities of employees under their immediate control.

B. Supervisors in each organizational component are responsible for conducting line inspections of uniformed personnel and sworn non-uniformed personnel within their organizational component and the correction of any deficiencies. See GO 527.3.B.5 for further.

202.4 ADMINISTRATIVE REPORTING PROGRAM

The University of Chicago Police Department uses a computerized Police Records Management System to store and retrieve data. The Records Management System provides statistical and data summaries of Departmental activities. Administrative reporting is accomplished through the completion and distribution of the following reports:

A. End of Shift Reports.
End of Shift reports are a summary of the activity occurring during the previous shift. End of Shift reports are done by the Squad Captain or Shift Supervisor and disseminated via email to Sergeants and above, the Crime Analyst, the Records Manager and the Emergency Communications Center Manager.

B. Compstat Weekly reports.
Compstat weekly reports are comprehensive reports contributed to by all segments of the Department and put out by the Crime Analyst, to all sworn personnel and some non-sworn supervisors and managers.

C. Daily and Weekly Crime Analysis Summary reports.
Daily and weekly crime analysis summary reports are put out by the Crime Analyst to include violent crime statistics, and daily activity, to different groups within the Department.

202.5 FORMS ACCOUNTABILITY

The Professional Standards Commander, or designee, is responsible for all Department forms, including a record of all forms and form numbers. Forms management is designed to ensure that only necessary and essential forms are retained in use and that all others are eliminated.

A. The Professional Standards Bureau shall be responsible for the development and modification of all forms used by the Department.

B. The review process for new or modified forms shall include personnel in the components who will use and process the forms. All new or revised forms will be reviewed by the Policy Review Committee.

C. The final authority over all new or modified forms shall rest with the Chief of Police or designee.

202.6 ACCREDITATION REPORT/REVIEW SYSTEM

The Professional Standards Commander will be responsible for overseeing the Department’s efforts regarding performing and documenting activities mandated by applicable accreditation standards. Performing and documenting these activities, however, are the responsibility of all Department personnel. An electronic task management system will be utilized for providing follow-up notices and tracking the submission of accreditation materials.

A. Time sensitive accreditation standards requiring periodic reports/submissions will be closely monitored using task management software. Follow-up notices will be generated and disseminated to ensure timely submissions.

B. Periodic updates to accreditation files may be done by supervisory personnel who specialize in the topic of particular standards (forensics, records, etc.).

C. Reports or notifications of incidents which are documented on a per-occurrence basis (pursuit, use of force, strip search, etc.) will be forwarded to the Accreditation Manager.

202.7 COMPUTER SECURITY

A. All software used on Department computer equipment must be approved by, and installed by, University IT.

B. External data and data storage devices of unknown or suspicious origin will be checked by University IT and approved for introduction into Department computer systems hardware, prior to use in a Department computer.

202.8 USE OF MOBILE DATA COMPUTERS (MDC/MDT)

A. The Department/IT will maintain and keep updated a list of authorized users for each system.

B. As a rule, no extended keyboard entry shall be performed on an MDC when the vehicle is in motion except in cases of extreme emergency. Extended keyboard entry shall only occur when the vehicle is stopped OR the MDC operation is being done by someone other than the driver. Single key strokes, such as those to change status and view screen, are not considered extended keyboard entry.

C. Employees will utilize the MDC to update all status changes.

D. No improper language, including vulgarity and profanity, or other derogatory, insulting, or offensive communication will be transmitted over any MDC or computer work station.

E. Transmissions by MDC are for work-related messages and transmissions only. Examples include assignment of a call for service, status checks, beat information or, in some situations, personal or emergency notifications. All such messages shall be professional and appropriate. Supervisors are responsible for reviewing the electronic MDC transmissions of their personnel, including CAD dispositions for Calls For Service.

F. All software used on Department MDCs must be approved by, and installed by, University IT. Unauthorized installation of software programs or other files, may be cause for disciplinary action.

G. Current software running on Department MDCs, desktop or handheld computers will not be manipulated or altered without the approval of University IT.