

**Albany Police Department  
Computer and Technology Unit  
Albany Police Public Safety Network  
Third Party User Agreement**



**NETWORK ACCESS**

The Albany Police Department has established access control standards for information systems. These standards have incorporated policies that balance restrictions and prevent unauthorized access to meet business needs. Access to all systems must be authorized by the Computer and Technology Unit. Access rights and privileges are to be recorded in an Access Control List. All records associated with the access control lists are regarded as highly confidential and safeguarded accordingly. However, all records associated with access control lists are subject to department policies and investigations as appropriate.

Equipment is always to be safeguarded appropriately, especially when unattended. Unauthorized access to an unattended workstation can result in harmful and fraudulent entries. It may also lead to deletion of data or the modification of system files.

User ID's used as passwords may invite hackers or fellow employees to attempt logins. Do not give your password away or write it down. A combination of letters and numbers is preferable and at least 6-8 characters are recommended. Although the Computer and Technology Unit may assign an initial password for any given system, all efforts must be made to change the password immediately.

**COMPUTER AIDED DISPATCH SYSTEM / RECORDS MANAGEMENT SYSTEM ACCESS NOTIFICATION**

The **CAD/RMS** system is restricted to authorized personnel for official Police, Fire and Emergency Medical Services use. The data and records in the **CAD/RMS** system are confidential. Unauthorized access of the database, tampering with or changing system files, without prior authorization from the Supervisor of the Albany Police Department Computer and Technology Unit, can subject a person to criminal prosecution, departmental charges, or having access suspended from the system.

Dissemination of any system information to another person is prohibited unless they are acting in an official capacity and are authorized through official channels. Authorized users will be assigned a **USER ID** and a **PASSWORD**. Upon initial login, the user must change the password to a secret password. **CAD / RMS requires 6-8 characters with at least 1 numerical value**. Failure to do so will prohibit the user from logging on.

To secure against someone using a session logged into under your **user ID**, you must either **"END"** your session **OR** verify that your relief has successfully changed the user ID with the **"LOG"** function. **IF YOU LEAVE A WORK STATION WITH THE "LOG" COMMAND STILL ON YOUR SCREEN, ANOTHER PERSON CAN CONTINUE USING YOUR ID.**

I, \_\_\_\_\_, hereby acknowledge that I have read the foregoing Department of Public Safety Policy on the use of resources via the Albany Police Department's computer network, Computer Aided Dispatch System, and that I fully understand the contents of this policy, and that I will comply fully with its provisions.

Agency: \_\_\_\_\_ Name: \_\_\_\_\_

Supervisor Name: \_\_\_\_\_ Signature: \_\_\_\_\_

Phone Number: \_\_\_\_\_ Phone Number: \_\_\_\_\_

Date: \_\_\_\_\_ Date: \_\_\_\_\_

I request access to the following APD systems:

- CAD / RMS
- eReporting
- License Plate Reader
- SSL VPN / Capsnet Web
- SSL VPN / Appsnet Web

Please Fax this form to (518)447-8762  
And MAIL the original to:  
Computer and Technology Unit  
165 Henry Johnson Blvd  
Albany, NY 12210

Any questions can be directed to [ctu\\_staff@albany-ny.org](mailto:ctu_staff@albany-ny.org) or (518) 462-8018

---

For Computer & Technology Unit Only

CTU Supervisor Signature & Date: \_\_\_\_\_  
(Signature) (Date)

User will receive access to:

- CAD / RMS \_\_\_\_\_
  - eReporting \_\_\_\_\_
  - License Plate Reader \_\_\_\_\_
  - SSL VPN / Capsnet Web \_\_\_\_\_
  - SSL VPN / Appsnet Web \_\_\_\_\_
- (UserName) (Password)