

CENTRAL COAST REGIONAL DISTRICT  
POLICIES

---

**A-3 - Office Security & File Security**

**Preamble:** There is a demonstrated need for file and office security to protect the public records and assorted documentation, from wilful or accidental loss.

**Policy:** That all original primary documents be kept in a fire proof security cabinet(s) of sufficient capacity for safekeeping. . That the corporate seal, in-office cash or monies, and other articles of public value be kept in a cabinet and locked at all times and that access to the security cabinet(s) be the responsibility of one designated staff member. That the staff member is to keep the key(s) or combination with them at all times with a duplicate key(s) or combination to be stored in a safety deposit box at the local financial institution.

And further, that all files of a confidential nature be stored in a locked cabinet(s) and that access to the cabinet(s) be the sole responsibility of the CAO or CFO.

And further that all electronic data be backed-up daily to an external storage device. See Policy A-27 Disaster Recovery Plan – Information Technology, for more information.

And further, that all computer access be protected by separate passwords and that all confidential electronic data be protected by a secondary password to be put in place by the CAO or CFO. .

And further, that the office, is not to be occupied by any person or persons except where a staff member or regular personnel is present.

And further, that only staff and regular personnel maintain key access to the building and that the Administrative Assistant, or the last member to leave the building, ensures that all doors and windows are secured with blinds and interior doors in the closed position.

Date: September 14, 1993  
Amended: February 13, 1996, November 15, 2012, November 14, 2013  
Amended: July 9, 2015