3-07/210.25 - Security

Only Department-authorized persons or other persons authorized by Data Systems Bureau may access the Department IT systems. Those authorized will be assigned a logon identification code (i.e., USERID or ID). Only the authorized owner of the ID is permitted to use the ID. Those assigned an ID will also be required to select a password. Authorized persons shall not disclose their computer passwords to another person, except as required under this policy. Authorized persons are responsible to keep their passwords secret and to change them if compromised. Any electronic communications sent using an authorized persons' USERID and password is prima facie evidence the employee assigned the USERID and password generated the communications.

Authorized persons shall not share common USERIDs and passwords for any computer system, except as required for training or as specifically authorized by Data Systems Bureau. Any person who has knowledge of individuals who are sharing common USERIDs and passwords shall immediately notify their unit commander, in writing, with a copy to Data Systems Bureau. Authorized persons shall have only one network, e-mail, and fax account unless authorized by Data Systems Bureau. Only Data Systems Bureau shall authorize IT systems access and USERIDs.

Passwords must adhere to the standards set forth in the Security Standards, which may be found on the intranet under Policy/Standards/Guides on the Data System's Bureau intranet web site.

In order to prevent unauthorized access to the Department IT systems or misuse of information maintained by the Sheriff's Department, authorized persons must comply with the IT policies, standards, and guidelines which may be found on the Intranet under the Policy/Standards/Guides on the Data Systems Bureau Intranet web site.

Those users designated as "owners" of groups (e.g., security groups, distribution groups) shall periodically review membership of the group. Owners shall appropriately remove membership when a user's role no longer meets "right to know/need to know" criteria.

Authorized persons shall immediately report to their unit commander, in writing, any violations of electronic communications policy as set forth in the Manual of Policy and Procedures, section 3-07/210.25, section 3-07/210.55, and section 3-07/250.00.