3-07/220.00 - Prohibitions

Authorized persons shall not add, alter, copy, damage, delete, move, modify, tamper with, or otherwise use or affect any data or software, computer, computer system, or computer network in order to either:

- Devise or exclude any scheme or artifice to defraud, deceive, destroy, or extort;
- Wrongfully control or obtain money, property, or data;
- Disrupt or cause the disruption of computer or network services, or deny or cause the denial of computer or network services to an authorized user of a Department computer, computer system, or computer network; and
- Assist in providing access to unauthorized persons to any data, software, programs, computer system, or computer network.

  Unless specifically authorized by Data Systems Bureau, authorized persons shall not install, connect to, move, change, modify, disconnect, or tamper with any data circuit, router, switch, hub, data jack, data cable, server, or other data communications equipment or software or assist any unauthorized person in gaining access to data circuits, routers, switches, hubs, data jacks, data cables, servers, or other data communications equipment or software.

  Authorized persons shall not do any of the following without the required authorization:

- Access or allow access to another to obtain, alter, or prevent access to stored electronic communications or data;
- Use electronic communications to capture or open electronic communications of another, or access files without permission of the owner;
- Damage hardware, software, or other communications/body-worn camera equipment or interfere with functionality;
- Attempt to breach any security measures on any electronic communications system, or attempt to intercept any electronic communication transmission;
- Modify or delete any file, folder, or system audit, security, or ownership records or time stamp with the intent to misrepresent true system audit records;
- Access the files belonging to another for non-business purposes;
- Use someone else's USERID, password, or access another person's files, or retrieve stored communications without authorization;
- Modify the hardware or software configuration on any computer;
- Use electronic communications to transmit (upload) or receive (download):
  - Any communication violating any applicable laws, regulations, or policies;
  - Proprietary or confidential Department information;
  - Chain letters; and
  - Material that would be offensive to a reasonable person;
- Transmit any electronic message in violation of file size restrictions;
- Use Department computer equipment or network to send or receive electronic communications for non-Department business;
- Use computers, networks, or electronic communications to infringe on the copyright or other intellectual

property rights of the county or third parties;

- Send or receive commercial software in violation of its license agreement;
- Copy personal files, programs, or images into any Department computer without authorization from their unit commander;
- Send anonymous messages or represent themselves as someone else, real or fictional, or send messages or images which are defamatory, fraudulent, threatening, harassing, sexual, or contain derogatory racial or religious content;
- Establish any hidden or misidentified links on any web page;
- Send or forward messages which have been altered in order to deceive the receiver as to the original content;
- Use Department computers, networks, software, electronic communications, or body-worn camera equipment for personal financial, commercial, political, or other personal use;
- Use electronic communications to intimidate, embarrass, cause distress, or otherwise force unwanted attention upon others or to interfere with the ability of others to conduct Department business or create a hostile work environment;
- Use electronic communications in competition with commercial services to individuals or organizations outside the Department;
- Use electronic communications for the purposes of gambling, including but not limited to, lotteries, sports pools, and other personal wagering; and
- Give out employee personal information such as home address and/or telephone numbers.