

---

# Butte County Mosquito and Vector Control District

## POLICY MANUAL

**POLICY TITLE:** Computer Security  
**POLICY NUMBER:** 3010

**3010.1 Purpose.** The Butte County Mosquito and Vector Control District seeks to ensure that computer security procedures for District personnel who are issued desktop or laptop computers and/or internet accessible devices and who may handle sensitive or important information to the operation of the agency.

**3010.2 Scope.** This program applies to all employees who are issued desktop or laptop computers and/or internet accessible devices.

**3010.3 Responsibilities.**

**3010.3.1** The District Manager approves all purchases of desktop or laptop computers and/or internet accessible devices for use by District personnel.

**3010.3.2** The Assistant Manager is responsible for assigning laptop computers to personnel for District use and is responsible for enforcement of this policy.

**3010.3.3** Each employee issued a desktop or laptop computer and/or internet accessible devices is responsible for understanding and following the requirements of this policy.

**3010.4 Computer Security.**

**3010.4.1** District shall have and maintain a network firewall.

**3010.4.2** A password will be required to open programs on laptop computer.

**3010.4.3** Any software installed on the laptop computer must be pre-approved by the Assistant Manager.

**3010.4.4** Internet access may only be made through the District's network server. The laptop computer may not be used to access the Internet via an employee's personal Internet account. Employees working remotely must access Internet through a secure network.

**3010.4.5** The laptop computer may be transported between the main District office and substation and then from either District office to the field location at which the employee is assigned to work via a District vehicle. If the employee at any time leaves the vehicle unattended, the laptop computer will be stored out of sight in a locked compartment or secured to a vehicle laptop mount.

**3010.4.6** All electrical, civil and/or mechanical schematics, drawings, photos and database records will be stored in electronic format on the District's network computer. Only those schematics, drawings, photos or maintenance database records necessary for the work being conducted at the given field location may be downloaded and temporarily stored on the laptop

computer's hard drive. Upon completion of the field assignment, all revised files will be uploaded onto the District's network computer and all temporarily stored files will be deleted from the laptop computer's hard drive.

**3010.4.7** Any desktop or laptop computer may not be removed from the District's service area without prior approval of the District Manager.

**3010.5** Compliance. The Assistant Manager will periodically check all desktop or laptop computers to ensure that no critical infrastructure information or other sensitive data is being stored on the computer's hard drive. Personnel found to be in violation of this policy will be subject to disciplinary procedures in accordance with Policy 7260.