

| | |
|----------------------------------|--|
| C D I | I n f o r m a t i o n S e c u r i t y P o l i c y |
|----------------------------------|--|

To: ITD Staff

No.: ISO-06

From: Information Security Office (ISO)

Issued: August 1, 2004

Subject: Logging Policy

Expires: When Superseded

Policy

The Information Technology Division (ITD) will log, monitor and analyze California Department of Insurance (CDI) network traffic which includes Internet e-mail, personal computer logs, and all web site communications and related activities. CDI cannot guarantee privacy in the use of these resources. ITD will also review all virus and firewall logs no less than monthly. All security related events on these critical and sensitive systems shall be logged and the audit trails saved as follows:

- All security related logs will be kept online for a minimum of one year;
- Daily incremental tape backups will be retained for at least one month;
- Weekly full tape backups of logs will be retained for at least one month;
- Monthly full tape backups will be retained for a minimum of one year;

Purpose

To protect the CDI network from inappropriate or illegal use of state resources and ensure that the critical CDI network systems logs are monitored and analyzed.

Procedure

ITD will develop and implement procedures to ensure logging and monitoring activities are common practices within CDI. ITD will perform network monitoring at least weekly to ensure that the network is functioning properly and to determine bandwidth and protocol usage. The ISO is responsible for coordinating a follow up review of any abnormalities in the logging process, pursuant to Administration Bulletin # 03-06.

Inquiries

Please contact the ISO at 916-492-3256 or 916-492-3353 if you have any questions regarding this policy.

Archie Alimagno, Information Security Officer