

SYSTEMS AUDIT CONTROLS PROCEDURE

I. AUDIT CONTROL AND REVIEW PLAN

- A. Identify the components of the information system environment that will record audit trails and be used in the internal audit process in the Audit Control and Review Plan. These components may include perimeter devices (e.g., firewalls, network intrusion detection systems, routers, switches, VPN appliances, and guard devices), servers (e.g., web, application, file, print, and database), workstations, and applications.
- B. Define the events to be audited for the information system component identified above (e.g., logins, file access, and data modification).
- C. Determine the scope of the information that is to be recorded for both information at rest (storage) and information in transit (transmission).
- D. Enable the auditing mechanism on the information system identified in Section A. above.
- E. Determine the roles and responsibilities of Workforce Members for the operation of the auditing mechanism and the review of the audit reports. The monitoring and review of audit trails and internal audit reports must be assigned to a person who does not have responsibility for system operations.
- F. Determine the frequency and content of audit reporting.
- G. Escalate potential security incidents or unusual logged events to the DMH Chief Information Officer (CIO) or his/her designee.

II. MANAGING THE SECURITY OF AUDIT TRAILS

Reasonable safeguards must be maintained to ensure the confidentiality, availability, and integrity of audit trails and internal reports and to prevent unauthorized access. These safeguards must include, but not be limited to, the following:

- A. Password protected access to audit logs and internal audit reports, including the use of file integrity checkers.
- B. Regularly backing up audit logs and storing them in fire resistant, offsite, locked containers. The process of audit trails and internal audit reports must be consistent with the data backup procedures in DMH Policy No. 550.03, Information Technology (IT) Contingency Plan.
- C. Limiting the number of persons necessary for monitoring and reviewing audit trails and internal audit reports.