b. User IDs or other identification mechanisms

c. Success/failure of system access attempts

d. Source and target network addresses and protocols details

e. Action that occurred.

7. The University shall retain event logs for 3 years with at least 3 months available for 'online' access or as required by federal, state, or local laws and organizational policies.

8. Logging data shall be routinely reviewed and analyzed by trained personnel. The frequency and nature of log monitoring and review depend on the risks to the relevant computer system and underlying data. They shall be commensurate with a particular system's profiled data classification category.

    f. All security events and operational logs shall be reviewed to detect deviations from policy and to test the effectiveness of access control and security mechanisms.

    g. Review all events to detect unusual activity and suspicious events.

    h. Review all application and system events to discover errors and performance issues.

9. The log management system and logging data shall be protected against unauthorized tampering, modification, and destruction. Access to log files and logging data shall be audited, monitored, and restricted to need-to-know personnel.

10. Once logging data has reached the retention schedule, it shall be securely purged and eliminated unless it needs to be retained for legal or eDiscovery purposes.

11. IT Security personnel shall monitor log management processes and systems and conduct audits, at least quarterly, of the log management system.

B. Roles and Responsibilities

1. The Information Security Office (InfoSec) is responsible for protecting the log management system, monitoring activity logs, and auditing the log management system.

IV. DEFINITIONS

– a file that stores a record of the events that occur in a computer system.

– information contained within log files.