Log File Access and Retention Policy

Date Established: 7/14/2010
Date Last Revised: 7/14//2010
Date Posted to Library: 9/10/2010
Category: IT Policy
Responsible Office: CIO Office

Summary

This policy identifies the retention and destruction rules for system logs, also known as log files,[1] on servers and networked devices that are managed by central IT. Log files are stored for the exclusive use of the central IT system administration staff for specific business reasons or to satisfy legal requirements. Log files are considered to be confidential and are subject to the privacy requirements of this policy and the retention guidelines in the *Retention Guidelines for Log Files* and are destroyed after their business use is completed.

Policy

POLICY STATEMENT

Log files created by UB's central IT servers record only basic information about the activity supported through these servers. Log files are stored for the exclusive use of the central IT system administration staff for specific business reasons[2] or to satisfy legal requirements. Log files are classified as protected data and are subject to the privacy requirements of this policy, the Data Access and Security Policy, the retention guidelines in the *Retention Guidelines for Log Files*, and are destroyed after their business use is completed.

Central IT retains these records or logs for a time period specified in the *Retention Guidelines for Log Files*. All logs are considered to be confidential and protected data, and central IT takes active measures to prevent unauthorized access during the retention period.

BACKGROUND/REASON FOR POLICY

Log files on servers and networked devices managed by central IT are classified as protected, non-public data. This policy implements UB's privacy and data protection rules for the collection, access to, and retention of server log files. In setting the retention period central IT has considered a variety of competing interests, including the need to maintain operational reliability, the desire to reduce storage costs, and the desire to limit log retention to reduce opportunities for inadvertent disclosure of data.

APPLICABILITY

This policy applies to log files on servers and networked devices managed by central IT.

---

[1] Log files are created automatically during system operation and contain entries about the events that happened in a system. They are vital for systems troubleshooting and analysis. For example Web Servers automatically save usage and activity information such as the date, time, IP address, HTTP status, bytes sent, and bytes received.

[2] Business reasons include troubleshooting, collecting statistics on usage and activity, billing, documentation, and forensic investigation.

DEFINITIONS

Log files - Records (text files) that are created automatically during system operation and contain entries about the events that happened in a system. They are vital for systems troubleshooting and analysis. For example Web Servers automatically save usage and activity information such as the date, time, IP address, HTTP status, bytes sent, and bytes received

RESPONSIBILITY

Chief Information Officer

The CIO or his designee approves requests for access to server log files.

PROCEDURES

ACCESS TO LOG FILES

While the usage logs covered under this policy do not contain personally identifying information as addressed by recent federal and New York State laws, the logs are classified by University at Buffalo as protected data. The reason for this is that the log files used in conjunction with other information that central IT has in its custody may allow us to associate specific information on the use of a service, such as specific Web page access, with a given individual's computer.

The CIO Office will comply with a court order or valid subpoena that requests the disclosure of information contained in usage logs. Failure to comply could have serious consequences for the individuals involved, the CIO Office, and the University at Buffalo.

RETENTION OF LOG FILES

Log file retention times are specified in the *Retention Guidelines for Log Files*. If a log file contains relevant information that is useful for future reference, a pending transaction, or as evidence of a management decision, it should be retained. If a log file is needed for these purposes, it is the responsibility of IT staff to move these specific logs to another central IT-owned system prior to the destruction of the log (after it has reached its maximum retention time).

DESTRUCTION OF LOG FILES

Log files must be destroyed in accordance with the *Retention Guidelines for Log Files*. All original, backups, and copies of logs should be destroyed. For this reason, log files should not be backed up to removable media and should stay on the centralized log server or the local file system of the machine on which they are generated. In addition, care should be taken to exclude log files from computer disk images.

This policy recommends deleting log files as opposed to log entries. Logs should be destroyed in the most destructive and economical way available. Actual deletion method are specified in the *Retention Guidelines for Log Files*.

Contact Information

For more information about this policy, contact the

Office of the CIO
517 Capen Hall
University at Buffalo
716-645-7979

Related Information

University Documents:

Retention Guidelines for Log Files
Data Classification Standard
Data Access and Security Policy

Other Documents:

Title of Related External Document Linked when possible

Related Links:

Linked Title of Related Informational Item