Protect: Secure Log Storage

`

COST: **$$$**$ IMPACT: **HIGH** COMPLEXITY: **LOW**

2.U: Does the WWS protect security logs from unauthorized access and tampering?

Recommendation: Store security logs in a central system or database that can only be accessed by authorized and authenticated users.

Why is this control important?

Protecting security logs is important because if an attacker compromises a system, they may modify or delete the logs to destroy evidence and cover their tracks. This step helps to make sure that your WWS protects its security logs from unauthorized access and tampering.

Detecting and responding to a cyberattack becomes much more difficult without trusted log data to track what an attacker does on a computer system.

Implementation Tips

Store logs for a period that considers WWS policy, state regulations (if any), and cyber risk. A common log retention period is six months.

Ensure security logs are part of your WWS's standard backup procedures so you can review the logs even if the source is no longer available.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control family AU and AU-9 (page 74) for more information on “Audit and Accountability” and “Protection of Audit Information."
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Additional Guidance

- ✓ Storing logs in a central system or database can be achieved using Security Information and Event Management (SIEM) systems, further covered in Factsheet 2.T. In addition to ease of log collection and analysis, SIEM tools also enable the System Administrator to set access permissions by user, referred to as Role-Based Access Control (RBAC). When storing logs in a central location with or without a SIEM tool, ensure that each user has an individual account to access log storage (i.e., SIEM Tool, Log Database, or Log Server).
- ✓ Regardless of how the WWS stores the logs, it should back them up to a secondary storage location on a regular schedule. A common backup schedule is daily. Regulatory, operational, and technological requirements and constraints often determine log retention periods; however, a common log retention period is six months. A longer log retention period is generally better than a shorter one as responders will have more evidence to review when investigating a potential cyberattack.

NIST Policy Template Guide Protect: See Security Logging (4.5b) Log Access and Use (Revision 5) Security and Privacy Controls for Information Systems and Organizations:

`

Documented SOP for protecting security logs. *https://www.cisecurity.org/wp-content/uploads/2020/06/Security-Logging-Standard.docx*

WaterISAC's 15 Cybersecurity Fundamentals: See page 31 for more information on "Logging and Auditing." *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

Microsoft Learn – Set up or customize server backup: See this resource for more information on how to configure backups for log storage locations. *https://learn.microsoft.com/en-us/windows-server-essentials/manage/set-up-or-customize-server-backup*