IT LOGGING STANDARDS

Contents

Document History

First release date	18th May 2017
Approved / Reviewed by	Approved by ITS Solutions Architecture Group
Owner	IT Security / Stephen Shaw
Intended audience	UoW IT System & Application Owners
Restrictions	UoW IT Teams and Governance
Last revision date	5th November 2019
Next review date	December 2021
Version number	1.2

1. Overview

Logging from IT systems, applications and services can provide key information and potential indicators of service affecting events, cyber security incidents and compromise.

Although logging information may not be viewed on a daily basis, it is crucial to have appropriate logs retained from a response, investigation and forensics standpoint.

Legislation, formal audits and IT Security team requirements have highlighted the need to produce a formal document relating to effective collection, treatment and retention of these system logs. This policy states the requirements and covers a process for compliance exceptions.

2. Purpose

The purpose of this Policy document is to introduce and enforce procedures to identify specific requirements that information systems must meet in order to generate and store appropriate logs for retention.

3. Scope

This Policy applies to all University IT Systems, onsite or hosted that store or process information classified as Protected, Restricted or Reserved under the University Information Security Framework.

This Policy applies to any system, associated with the above scope statement that accepts network connections, provides application hosting or makes access control (authentication and authorisation) decisions.

This Policy is limited to system logging and does NOT cover Data Protection, Monitoring or Interception.

4. General Requirements

All systems within scope must record and retain logging information.

Typical systems would include; Windows, Linux, Unix and VMware Servers, associated Mail, Database and Applications, Workstations, Anti-Malware, Active Directory, Radius, DNS, DHCP, VPN, Firewall, Networking and Telecoms equipment.

The log information should be sufficient to answer the following types of questions:

What?

- Type of event;
- Severity of event e.g. {0=emergency, fatal, error, warning, info, debug, trace};
- Security relevant event flag (if the logs contain non-security event data too);
- Description;

When?

- Log date and time (International format ISO 8601) YYYY-MM-DDThh:mm:ss.sTZD;
- Event date and time - the event time stamp may be different to the time of logging;

Who?

- Source address e.g. user's device/machine identifier, user's IP address, MAC address;
- User identity (if authenticated or otherwise known);

Where?

- Application identifier e.g. name and version;
- Application address e.g. cluster/host name or server IPv4 or IPv6 address and port number, workstation identity, local device identifier;
- Service e.g. name and protocol;
- Window/form/page e.g. entry point URL and HTTP method for a web application, dialogue box name;
- Code location e.g. script name, module name;

Each system must synchronise its time clock with a reputable clock source and where feasible, the University NTP clock source (ntp.warwick.ac.uk) to ensure log events from different systems can be correlated. Co-ordinated Universal Time (UTC) is the standard strongly preferred.

All administration level access to each system must use accounts, which identify individual administrators or system processes. Generic or default accounts shared by multiple administrators or processes should not be used.

The logs generated from each system must provide enough information to be useful for the IT Security team and the IT System or application owners.

Access permissions to local and central logs must be managed such that unauthorised users cannot modify or interrupt the processes used to create or store log files on systems.

Log files stored in the central logging system must be set to restrict access privileges for each set of system logs, to authorised accounts and users.

5. Activities to be logged

IT system and application owners are expected to assess if systems falling into their areas of responsibility are in scope as detailed in section 3.

Logs must be set to capture security and event information as a minimum. If feasible, log information must be created whenever any of the following activities are performed by the system:

- Create, read, update, or delete information, including confidential authentication information such as passwords;
- Initiate or accept a network connection;
- User authentication and authorization, such as user login and logout;
- Password resets and credential recovery mechanisms such as those used in Web SSO;

- Grant, modify, or revoke access rights, adding a new user or group, changing user privilege levels, file permissions, database object permissions and firewall rules;
- Configuration changes, including installation of software patches and updates,
- Application process start-up, shutdown, or restart;
- Application process abort, failure, or abnormal end, resource limit or threshold (i.e. CPU, memory, disk space), failure of network services such as DHCP or DNS, or hardware fault;
- Unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database
- Detection of suspicious / malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-malware system.

6. Formatting, Transmission and Storage

The IT system must support the formatting and storage of logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following:

- Operating system event logs;
- Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols;
- Logs stored in an ANSI “standards based” SQL database that itself generates audit logs in compliance with the requirements of this document;

In addition to logs, which are held locally by each system, the log information required by this Policy must be passed simultaneously to the IT Services Central Log Store.

Where possible, any data transmitted between log sources and a centralised log store must be secured to prevent unauthorised modifications. Those devices and log agents not supporting encrypted communication channels natively and using plaintext protocols can be protected with additional layers of encryption such as Internet Protocol Security (IPsec) tunnels.

For log data sent to the centralised location, security measures such as digital signing or encryption should be implemented to ensure the integrity of this data, although for large volumes this may have unacceptable efficiency or administrative overheads and an exception will need to be requested.

Local, system storage must be managed by the system owner to ensure enough capacity has been assigned for the raw log file retention period to be 6 months or for as long as is feasible.

7. Retention

All logs required by this policy and where feasible must be retained for a minimum of 6 months.

Any logs related to this Policy and which contain Personal Data as defined by the University Data Protection Policy, must not be retained for longer than necessary, with 12 months as the maximum default period unless explicitly required for a specific purpose (such exceptions should be documented).

8. Policy Compliance

It is accepted that full Policy compliance across the institution may take some time and require a phased approach, however it is expected that all relevant IT systems, in all departments will comply.

Priority will be determined on the classification of data held within each system, the usefulness of the log data to the IT Security team, and then the feasibility of collecting such log data.

The IT Security and Information Security teams will verify the resultant compliance to this policy through various methods, including but not limited to, system native log data requests, central logging service analysis, business tool reports, internal and external audits, and feedback to the policy owner.

9. Related Standards, Regulations, Policies and Processes

- Payment Card Industry Data Security Standard (PCI DSS)
- UoW Information Classification and Handling Procedure
- UoW Data Protection Policy
- General Data Protection Regulation (GDPR)
- Cyber Essentials Certifications