ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-018 – Monitoring and Logging Policy

Author:	Craig Douglas
Date:	14 June 17
Document Security Level:	**PUBLIC**
Document Version:	0.92
Document Ref:	EA-POL-018
Document Link:	
Review Date:	June 2018

EA-POL-018 – Monitoring and Logging Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	Craig Douglas	Enterprise Architect	Initial Document	10/06/2016			
0.90	Paul Ferrier	Enterprise Security Architect	Various updates	10/08/2017			
1.00	PF	ESA	Final amendment before publication	17/08/2017 10:15	Paul Westmore	IT Director	17/08/2017 10:15

Table of Contents

EA-POL-018 – Monitoring and Logging Policy

Purpose

The University of Plymouth invests heavily in its Information Technology estate and processes a great deal of valuable and sensitive data upon it, as such the protection of this data from unauthorised access, theft and misuse is of paramount importance.

In order to comply with legal and regulatory requirements, as well as to provide assurance to University executives within the organisation, the monitoring (proactive) and logging (retrospective) of activities are required in order to understand and improve on the levels of protection surrounding the information.

The purpose of this policy is to establish and enforce practices for the monitoring and secure logging of system events across all systems which have a role to play in contributing to the successful execution of business functions throughout the University. The requirement for producing this policy and the statements within, is to ensure system and service owners are both aware and prepared for incidents as they arise, and are better informed to enable successful root cause analysis operations to be completed for both technological and security incidents.

Principles

P1. The University will monitor and log activities in order to protect our staff, students and partners, their devices as well as the information that they access. The intention of both monitoring and logging is not to be intrusive of legitimate work being conducted; however, to capture and retain this information in accordance with statutory obligations, log files must be generated and be made available for interrogation. The monitoring function will highlight any significant malicious activities and the logging function will only be used to retrospectively to diagnose any network or service problem or provide information to support an investigation.

P2. Activities that are logged will be kept secure and only accessible by appropriate staff. In order to maintain the confidentiality and integrity of the underlying data and to record what has happened, restrictions will be placed on who can access log files and these appropriate members of staff must be granted read only permissions. If greater access is afforded then the log files could be altered destroying any evidential trail that may later be required by the University or other regulatory authorities.

P3. Time synchronisation services will provide both accurate and consistent data for all systems to consume, this must be distributed from an industry accepted source. In order to preserve the timeline of events when a security incident occurs, collecting log files from multiple systems with inconsistent time can cause problems stitching the audit trail together. Time data will be distributed from dedicated servers to ensure consistency across the University's digital assets.

Goals

G1. To provide consistent evidence to support an investigation and remediation to prevent recurrence in the event of any system or service failure or data breach.

G2. To minimise inadvertent data loss and foster a culture of secure information handling.

G3. To prevent, where possible, malicious activities being carried out on the University's network.

G4. To provide consistent and accurate time to all digital assets that are connected to the University's network.

EA-POL-018 – Monitoring and Logging Policy

Objectives

O1. Provide a swift, effective and appropriately documented response to any failures or breaches of University systems, services or assets. **(P1, P2, P3)**

O2. Protect University data by preventing, where possible, malicious activities occurring. **(P1, P2, P3)**

Responsibilities

Role	Responsibility
SIRO	is responsible for all information and sets the acceptable level of risk of the University's informational estate.
IT Director	has delegated responsibility for the management and security of the University infrastructure, devices and systems provided internally or by its service providers; additionally, delegated responsibility to impose sanctions on devices for non-compliance with this policy is granted.
Faculties and directorates	have delegated responsibility to maintain secure systems, services and servers that they manage are producing relevant log files.
Enterprise Security Team	has responsibility for: • undertaking the creation of information security incident or investigation reports when required; • providing impartial adjudication where deficiencies in existing service provision are discovered and advising improvements to align with this policy; • defining University-wide policies to protect its systems, services and underlying data.
Everyone	has a role to play in information security including understanding the rationale behind monitoring and logging activity and the tight controls around its use.

Requirements under this policy

In accordance with the objectives stated in this policy, responsible parties must ensure the following in order to protect the University's data:

- Systems must generate log files to support investigations that are protected against unauthorised access or tampering;
- A University of Plymouth time service must be adopted by any centrally managed device connected to the network;
- Non-compliance with this policy should be reported to the Enterprise Security team for investigation and any remedial activities being drawn up.

Supporting documentation

EA-ISP-011 – System Management Policy
This sets out the governance surrounding the requirements for all services to log and be reviewed by appropriate members of staff.

EA-POL-017 – System and Service Investigations Policy
This sets out the governance surrounding activities required to aid in formal incident and investigations when required.

Sanctions

Failure to comply with this policy may result in either the device being placed into quarantine on the University network or, being disconnected in its entirety and potentially leading to disciplinary action for the responsible party.

Exception Management

Exceptions to this policy may be granted using the Enterprise Architecture Waiver Process and will be considered on merit as well as alignment with the overall architecture, business continuity requirements and other legislative requirements.