ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-018 - System and Service Investigations

Author: Paul Ferrier

Date: 10/06/2016

Document Security Level: **PUBLIC**
Document Version: 0.2
Document Ref: EA-POL-018 - System and Service Investigations
Document Link:
Review Date: tbc

EA-POL-018 - System and Service Investigations

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	Paul Ferrier	Enterprise Security Architect	Created the policy	10/06/2016			
0.2	PF	ESA	Updated following initial comments	09/01/2017			

EA-POL-018 - System and Service Investigations

Purpose

The purpose of this policy is to establish and enforce correct activities are performed in the correct order to allow for investigation into systems and services authored and maintain by Plymouth University in the event of a service affecting interruption.

Audience

This policy applies to all system, service and information asset owners, information asset stewards and administrators that store, process or transmit data for the University.

Scope

This policy applies to all University systems and services.

Policy

It is recognised that University systems and services must be resilient to component failure, in addition to this lessons must be learned and remedial action, if required undertaken, following any unplanned system or service episode. In this context an episode is defined as a period of time where a system or service is unavailable completely or constrained in its ability to function due to unknown or unforeseen events.

Formal security investigations will be conducted, at least initially, by the Security team within Strategy and Architecture, after each such episode. An output of the investigation is a document covering a comprehensive timeline of events and an executive summary for the dissemination to the management team.

The primary undertaking after the discovery of such an episode must be the collection of all relevant log files and their preservation for a formal investigation to occur. It is accepted that this will delay any remedial action to return the system or service to a working order, but this will ensure that the investigation is based on accurate information. With this in mind all relevant log files must be provided to the security team within **90 minutes** of the incident being opened.

Where necessary, engagement with experts from within or outside of the University will be sought to validate or interpret the collected information to provide an impartial perspective.

Any remedial activities, process reviews or improvements that are identified will be presented to the appropriate area of the business for enactment.

Failure to comply with this policy will lead to the issue being escalated to the IT Director through relevant management structures.

Exception Management

Any exceptions to this policy shall be at the discretion of the IT Director who will inform the Enterprise Security team in writing in order for the exception to form part of the evidentiary trail.

Supporting Documentation

This policy is supported by established Enterprise Architecture documents, namely:

EA-POL-018 - System and Service Investigations

EA-POL-013 – Business Intelligence Capability Policy

Principle 2: Compliance with Statutory Obligations

Principle 7: IT Responsibility

Principle 9: Data is an Asset

Principle 10: Data is Shared

Principle 11: Data is Accessible

Principle 17: Data will be Analysable