Incident Response Policy

The goal of this Incident Response Policy is to ensure that all units within IS follow a consistent approach to service restoration.

Campus notification must streamline our response and let our customers know what is happening in a timely and appropriate way to minimize the operational impact on affected groups.

INFORMATION SERVICES

DECEMBER 5, 2012

UPDATED MAY 30, 2013

Oregon State UNIVERSITY

Purpose

The goal of this Incident Response Policy is to ensure that all units within IS follow a consistent approach to service restoration and campus notification that both streamlines our response and lets our customers know what is happening in a timely and appropriate way to minimize the operational impact on affected groups.

Incident Response planning generally includes the following:

- After hours response plan.
- Predefined roles for effectively responding to a service outage.
- Standard communication and escalation protocol.
- Requirements for post event review and analysis.

Scope

This policy applies to all service-affecting incidents involving IT services provided by OSU Information Services.

This policy does not apply to Security Incidents. Please see the Information Security Manual section 502: Incident Response and Escalation.

Policy

All units within Information Services will have an established Incident Response plan that is followed whenever a service experiences an unplanned outage.

Minimum Standards:

1. After hours response plans must ensure that all priority 1 IT components have a designated contact that is shared with all other IS units to coordinate response.
2. Predefined roles must include a person designated to handle communications and to coordinate with other IS and University units as appropriate, to allow technical experts to stay focused on service restoration during an incident.
3. All priority 1 and priority 2 IT services must have a documented incident communication and escalation protocol.
4. Post review and analysis must be done for all service affecting incidents that involve priority 1 and priority 2 IT components. Analysis must include a formal incident report submitted to the Change Advisory Board and IS management that focuses on how similar events can be mitigated. The CAB shall provide additional feedback on the proposed mitigation(s) to IS Management as necessary.

Appendix A - Definitions

Incident - any unplanned service interruption is an incident.

IT Component - A system, device, application or document that is part of an IT Service.

IT Service - A customer-oriented offering and/or consumption of a technology-based transaction. For example, DNS is not considered to be an IT service, for it is not experienced by customers as a transaction or offering. Instead, it is considered to be an IT component.

Priority 1 IT Component - Crosses organizational boundaries, serving the business functionality of many units. Is critical to the ability of the University to meet its business and regulatory obligations, support the delivery of education, or administer research. Has strategic value to the campus such that encouragement of widespread use is desirable.

Priority 2 IT Component - The component is a feeder to Priority 1 components; or is a component that does not cross organizational boundaries, but is still critical to the ability of the University to meet its business and regulatory obligations.

Priority 3 IT Component - Any departmental IT component that supports the internal operations of any department or departmental function and does not cross organizational boundaries.

Security Incident - Any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples include attempts to gain unauthorized access to a system or its data, unwanted disruption or denial of service, unauthorized use of a system, or changes to a system without the owner's knowledge or consent. (Adapted from CERT definition at http://www.cert.org/csirts/csirt_faq.html.)