Provo City School District Technology Security Policy

Security Response Plan Procedure

Last Update Status: *Updated January 2015*

1. Overview

A Security Response Plan (SRP) provides the impetus for security and operational groups to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring operational groups to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

2. Purpose

The purpose of this procedure is to establish the requirement that all operational groups supported by the InfoSec team develop and maintain a security response plan. This ensures that the security incident response team has all the necessary information to formulate a successful response should a specific security incident occur.

3. Scope

This procedure applies any established and defined operational group or entity within the PCSD.

4. Procedure

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific operational group for whom the SRP is being developed in cooperation with the InfoSec team. Operational groups are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The operational group security coordinator or champion is further expected to work with the network security engineer in the development and maintenance of a Security Response Plan.

- Service or Product Description
  The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

- Contact Information
  The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product,

coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

- Triage
  The SRP must define triage steps to be coordinated with the security incident response team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

- Identified Mitigations and Testing
  The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

- Mitigation and Remediation Timelines
  The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.