

SAM – INFORMATION SECURITY
(Office of Information Security)

INCIDENT MANAGEMENT
(Revised 10/09)

5350

Agency management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. All agencies are required to report information security incidents consistent with the security reporting requirements in this policy.

Proper incident management includes the formulation and adoption of a written incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents.

In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences in the future.