

DoIT Service Catalog

Service: Computer Security Response

General information:

Computer security response is a service provided for receiving, reviewing, and responding to computer security incidents. Computer security incidents are defined as security investigations, computer forensics, assisting with the development of continuity of operations and disaster recovery plans (COOP/DRP), and incident response reporting.

Purpose:

Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. When computer security incidents occur, it is critical for an organization to have an effective way to respond. The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage and lower the cost of recovery. Taking a proactive approach to business continuity planning is the best way to minimize the impact of disaster on customers, employees, and stakeholders. Acting proactively minimizes loss of service and customer confidence.

Scope:

The computer security response service provides a Computer Security Incident Response Team (CSIRT) made up of computer security professionals trained to analyze electronic incidents. The Office of Information Security staffs five Information Security Officers trained in various security disciplines to cover a wide range of events. Events may include computer security investigations, computer forensics, assisting with the development of continuity of operations and disaster recovery plans (COOP/DRP), and incident response reporting. A CSIRT can be on-site and able to conduct a rapid response to contain a computer security incident and propose mitigation and provide response strategies.

Features:

Features covered under this service include a CSIRT that will work closely with the IT staff and Administration of an organization to ensure quality handling of an incident, perform computer investigations and/or computer forensics and assistance with the creation and testing of a Continuity of Operations plan and a disaster recovery plan (COOP/DRP).

Usage:

Services are provided to all state agencies and can be accessed Monday through Friday between the operational hours of 7:00 AM to 6:00 PM.

Value Proposition:

Services provided by DoIT's Office of Information Security are assessed into each Agencies budget therefore, there are no additional costs involved. In most organizations the IT staff has the responsibility to ensure the continued operation of the Agencies business, when an incident occurs the organization's IT staff does not always have the availability to bear the additional burden.

Future Plans: Growth projections. Future plans and associated value.

Options and Features		
Options/Choices	Cost	Notes
Computer Security Incident Response Team (CSIRT)	No charge beyond the assessment paid to DoIT	A CSIRT can be on-site and able to conduct a rapid response to contain a computer security incident, propose mitigation and provide response strategies.
Continuity of Operations & Disaster Recovery Planning (COOP/DRP)	No charge beyond the assessment paid to DoIT	Assisting with the development of continuity of operations and disaster recovery plans (COOP/DRP). Planning may include the following elements: essential functions; alternate facility(s); vital records, databases, and systems; orders of succession; delegation of authorities; resumption of services after an outage to a catastrophic outage.
Computer Security Investigation & Forensics	No charge beyond the assessment paid to DoIT	When a breach of trust occurs the collection and analysis of data from computer systems, networks, communication streams (wireless) and storage media in a manner that is admissible in a court of law must be done. Computer Forensics merge computer sciences and knowledge of the law to allow admissibility of evidence into the courtroom.

Access:

Service can be requested through a letter to the administrator of the Department of Information Technology.