

NAU Computer Security Incident Response Team (CSIRT) Mission

Mission

Computer security incident response has become an important component of information technology programs. Security-related threats have become not only more numerous but also potentially more damaging and disruptive. New types of security-related incidents emerge frequently. Preventative activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Information Technology Services is working with the University community to implement reasonable IT policies and procedures to secure computing and information services and to adequately protect the data security, confidentiality, and accessibility of our networked information without significantly compromising intellectual freedom.

Responsibilities of CSIRT

1. Identify categories of malicious activity that threaten the University's computing infrastructure. These categories are constantly evolving. They include, but are not limited to, the following:
 - a. Denial of Service attacks
 - b. Rapidly spreading or highly virulent malicious code (viruses, worms, trojans)
 - c. Unauthorized utilization of services by the University community members or others
 - d. Unauthorized access to protected computing and information services by University community members or others
 - e. Technical support for investigations approved by authorized University representatives, on behalf of the University
 - f. Ongoing threats not yet defined
2. Coordinate appropriate responses to counter malicious threats
3. Develop group-level response procedures so that there is archival documentation and clear understanding of roles across ITS and non-ITS groups
4. Periodically review processes utilized for Incident Response and make recommendations for improvements to the CSIRT Director, as appropriate
5. Be aware of developing security issues affecting computing and information services

Membership

The CSIRT is composed of representatives (and their alternates) from several major groups within ITS :

ITS Group	CSIRT Members
CSIRT Director	Harper Johnson
Network/Telecom Director	Matt McGlamery
Network Technology	Armand Ramirez, Matt Sells
MS Enterprise Network	Robert Lightner
Operations/Admin	Gary Kistner
Client Computing & Training Director	Ricky Roberts
Desktop Services	Dina Newsham, Julie Cislo and Michael Zimmer
Solution Center	Wendy Garrison, Dale Krause, Julie McCormick, and James Howington
Windows Systems	Fed Gallardo
Unix Systems	Lou Arminio, Tobias Kreidl
Academic Computing – Director	John Campbell
Academic Computing	Lanita Collette, Ray Gonzales, Ed Smith
Administrative Computing - Director	Pat Benson
Admin Computing	Sue Stefanko, Tina Thorstenson, Ankee Wu, Mike LaSpina, and Lucy Sullivan
Communications	
Type of Incident	Incident Coordinators
Email-Bourne Malware	
Malware other than Email-Bourne	
Network Issues	
Power Issues	

References:

**National Institute of Standards and Technology Special Publication 800-61:
Computer Security Incident Handling Guide
Brown University – Information Security Team**