

Security Incident Response Policy

The NOAO director shall appoint a CIO (Chief Information Officer) who will lead all incident response efforts.

- 1.** The CIO will be responsible (after consultation with NOAO management) for communicating the nature, severity and outcome of the security incident to the NOAO's Program Manager at the NSF. If necessary, further reports to the Program Manager will be made detailing progress on remediation efforts.
- 2.** The CIO will be the liaison with other organizations that become involved in the security incident.
- 3.** The CIO will be the sole voice for NOAO when communicating with the Press about the security incident.
- 4.** The CIO shall organize an Incident Response Group from the CIS departments of both hemispheres who will be charged with investigating security incidents and determining the actions needed to remediate the incident. Towards this end, the CIO will ensure that:
 - a.** several staff members in the group become trained in computer security forensics and join community security organizations such as REN-ISAC.
 - b.** an up-to-date list is maintained of contact information for the group including telephone and email facilities that are not part of the NOAO infrastructure.
 - c.** an up-to-date list is maintained of contact information for IT security people at peer institutions such as Gemini, NRAO and STScI.
 - d.** prior arrangements be made for leading the group in the event the CIO is absent from NOAO.

Revision History:

Created: 8 March 2010