



Technology Area

DEFINITION

| | |
|--------------------|--|
| <i>Name</i> | Incident Response |
| <i>Description</i> | Incident Response capability is a combination of technically skilled people, policies, procedures, and techniques that constitute a proactive approach to handling computer security incidents. |
| <i>Rationale</i> | Provides a consistent approach to handling security incidents. |
| <i>Benefits</i> | Consistent method of evaluation and associate metrics; decrease spread; minimize damage; fulfills risk mitigation; limits impacts; promotes awareness; proactively improves network assurance; increases communication |

ASSOCIATED ARCHITECTURE LEVELS

| | |
|---------------------------------|----------------------|
| <i>List the Domain Name</i> | Security |
| <i>List the Discipline Name</i> | Operational Controls |

Associated Compliance Components

| | |
|--|---|
| <i>List the Compliance Component Names</i> | <input type="checkbox"/> Incident Reporting Procedures <input type="checkbox"/> Incident Risk Level Assessment and Countermeasures |
|--|---|

Associated Product Components

| | |
|---|--|
| <i>List the Product Component Names</i> | |
|---|--|

TECHNOLOGY AREA DETAIL

| | |
|------------------------------------|---|
| <i>Supporting Documentation</i> | NIST Special Publication: SP-800-3 Establishing a Computer Security Incident Response Capability (CSIRC) – November 1991 |
| <i>Document Source Reference #</i> | http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf |

Standard Organization / Government Body

| | | | |
|----------------------------|--|----------------|---|
| <i>Name</i> | NIST | <i>Website</i> | http://www.nist.gov/ |
| <i>Contact Information</i> | National Institute of Standards and Technology (301) 975-NIST | | |

KEYWORDS

| | |
|----------------------|--|
| <i>List Keywords</i> | Incident reporting; intrusion detection; exposure; vulnerability; INFOCON; attack; incident impacts; defense; threat; risk; alerts; countermeasure; communication; denial of service |
|----------------------|--|

CURRENT STATUS

| | |
|-----------------------------------|--|
| <i>Provide the Current Status</i> | <input type="checkbox"/> In Development <input type="checkbox"/> Under Review <input checked="" type="checkbox"/> Approved <input type="checkbox"/> Rejected |
|-----------------------------------|--|

AUDIT TRAIL

| | | | |
|-----------------------------|------------|---------------------------------|------------|
| <i>Creation Date</i> | 12-19-2002 | <i>Date Accepted / Rejected</i> | 01-21-2003 |
| <i>Reason for Rejection</i> | | | |
| <i>Last Date Reviewed</i> | | <i>Last Date Updated</i> | |
| <i>Reason for Update</i> | | | |

