Intrada TECHNOLOGIES

IT Security Incident Response Plan

Both companies and individuals should have an IT Security Incident Response Plan. In a corporate environment, employees, vendors, and contractors need to know how to quickly report an incident to the correct people to respond and address the situation.

What is considered an “incident”?

An occurrence, condition, or situation arising in the course of work that resulted in or could have resulted in:

- Loss of data, compromise of account information, exchange of PII information, unauthorized network access,
- Phishing scam, email spoofing, or social attempt to collect information.

Building an effective IT Security Incident Response Plan involves a proactive approach. Intrada recommends the following:

1. Identify and appoint staff to a Center Security Team (CST).
2. You must communicate all incidents and situations immediately to the CST.
3. Engage in the response phase. Intrada breaks down the response phase into four sub-categories: detection, analysis, recovery and post-incident.

Response Phase 1: Detection

When and where the incident was first observed

Response Phase 2: Analysis

Determining the type of threat – accidental, internal, intentional and impact – from no effect to high

Response Phase 3: Recovery

Bringing affected systems back online and restoration or recovery efforts

Response Phase 4: Post-incident

Within two weeks of the incident the CST should discuss lessons learned

To report an incident, contact the Intrada Help Desk using the online Help Desk System or by calling 800-858-5745. The help desk team will route any incidents to the CST for review and follow-up.

31 Ashler Manor Drive
Muncy, PA 17756

intradatech.com
800-858-5745

Exceeding Expectations.