NWF Health Network
Policy & Procedure

Series:	900: Data Collection, Records and Reporting
Policy Name:	Information Technology (IT) Incident Response Policy
Policy Number:	921
Origination Date:	02/22/2024
Regulation:	CFOP 50-4 CFOP 50-5 CFOP 50-13 CFOP 50-14
Referenced:	900-921 x 1 NWFHN IT Disaster Recovery Plan

Policy

The purpose of this policy is to ensure that the Northwest Florida Health Network's incident response capabilities, used to monitor for security incidents have a maintained quality and integrity. The incident response capabilities determine the magnitude of the threat presented by these incidents, and to respond to these incidents. Without an incident response capability, the potential exists that in the event that a security incident occurs it will go unnoticed and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected.

Scope

This policy applies to all information systems and information system components of the NWFHN . Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, zero and thin clients, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

Governing Laws & Regulations Guidance	Section
NIST SP 800-171	3.6.1-3.6.3
The Florida Senate	CS/HB 7055: Cybersecurity

Policy Statements
Basic Security Requirements:

- An operational incident-handling capability will be developed and implemented for all organizational information systems that house or access the NWFHN's controlled information. The incident

response capability will include a defined plan and will address the seven stages of incident response:
    - Preparation
    - Eradication
    - Detection
    - Recovery
    - Analysis
    - Post-Incident Activity
    - Containment
- Incidents will be tracked, documented, and reported to appropriate officials and/or authorities both internal and external to the organization.

Derived Security Requirements:

- Incident response capabilities will be tested annually.
- To facilitate incident response operations, responsibility for incident-handling operations will be assigned to an incident response team.
- Incident response plans will be reviewed and, where applicable, revised on an annual basis. Review will be based on the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.

Policy Compliance

Violations of this policy will be treated like other allegations of wrongdoing at the NWFHN. Allegations of misconduct will be handled according to established City procedures. Sanctions for noncompliance may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing and networking resources and facilities; 2. Disciplinary action according to applicable City policies; 3. Termination of employment; and/or 4. Legal action according to applicable laws and/or contractual agreements.