DHHS INSIDER THREAT PROGRAM POLICY

Title:	**Policy NCDHHS Insider Threat Program**
Current Effective Date:	**January 2025**
Revision History:	**2/6/2023; 2/9/2023; 3/22/2023 Original**
Effective Date:	**May 1, 2023**

Overview & Purpose

This plan (ITP Charter) establishes the program policy and responsibilities for the North Carolina Department of Health and Human Services (NCDHHS) Insider Threat Program (ITP). The ITP will seek to establish an operating environment for individuals, facilities, information, equipment, networks, and systems secure from insider threats. The ITP will consult with records management, legal counsel, the privacy and security office to ensure relevant legal, policy, and security issues, including but not limited to the accessibility and use of Personally Identifiable Information (PII), are appropriately addressed.

An insider threat is defined as the potential that an employee, contractor, vendor, or other individual who has or had authorized access (Insider), to use their access, either maliciously or unintentionally, in a way that could negatively affect NCDHHS. This includes negative impacts to NCDHHS's mission, resources, personnel, facilities, information, equipment, networks, systems, or the security of NCDHHS. Insider threats risk harm to, among other things, sensitive or proprietary information, employee or customer PII, Protected Health Information (PHI), financial records, non-public records, or other critical assets, processes, or programs.

This ITP Charter accomplishes the following goals:

1. Deter, detect, and protect against espionage, theft, cyber threat activities, and sabotage conducted by or on behalf of outside organizations or persons; deter, detect, and protect against employees (both permanent and temporary), or other Insiders who pose a threat; deter, detect, and prevent against Insider threat actions; and mitigate the risks of Insider threat actions through administrative, investigative, or other preventive or response actions.

2. Gather, integrate, and report relevant and credible information that may indicate a potential or actual Insider threat to deter all active employees, contractors, vendors, and other third-party partners from becoming or continuing to be an insider threat.

3. Detect any person with authorized access to facilities, information, equipment, networks, or systems, who pose a risk to sensitive information (financial, business, personal data, etc.). Detection of these persons is based on their individual activities on systems and Insider indicators they may display.

4. Oversee and facilitate internal or external investigations in response to Insider-related issues/incidents and bring to closure by addressing and resolving.

5. Recover post-incident by conducting analysis to improve protective, deterrence, and detective measures in the future.

The framework of the ITP is centered around NIST SP 800-53: PM-12: Insider Threat Program and the National Insider Threat Task Force (NITTF). The primary mission of the NITTF is to develop an enterprise

wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of sensitive information from exploitation, compromise, or other unauthorized disclosure, considering risk levels, as well as the distinct needs, missions, and systems of individual agencies.

The NITTF leads the national effort to counter the insider threat and provides the foundations to safeguard critical assets identified by organizations.

Applies To

This ITP has scoped boundaries across several dimensions and has defined that scope as follows:

- Business Areas Included: The ITP applies to all business units and operating entities.
- People Included: All employees, contractors, and others with access to resources including facilities, information, equipment, networks, or systems.
- Data Classification Boundaries: Data classification levels subject to the scope of the ITP as defined by NCDHHS Policies and Standards Risk Types: The ITP scope will cover both intentional and unintentional threats. Risk Theme Boundaries (as part of Risk Analysis and Threat activities).

The ITP will focus on the following risk themes:

- Presumable Unintentional Data Leaks
- Data Theft
- Data Manipulation
- Reputational Damage
- Sabotage
- Advanced Persistent Industry Threats
- Emerging Threats
- Espionage

The following Insider Threat Themes are out of scope for the ITP:

- Physical Theft
- Workplace Violence
- Loss of Business Productivity
- Resource Misuse
- Product Sabotage
- Fraud

These out-of-scope areas may be included in future program expansion, etc.

Policy Requirements

The ITP is established to protect personnel, facilities, and systems from insider threats through the gathering, integration, and reporting of relevant and available information indicative of a potential or actual Insider threat. The Chief Risk Officer will designate an employee who is a senior official to establish and execute the ITP. The ITP will be in existence until formally discontinued by the NCDHHS Secretary in writing.

The following responsibilities are designed to enable the ITP team members/stakeholders to gather, integrate, centrally analyze, and respond appropriately to key threat-related information. The ITP will comply with the following minimum standards:

1. Shall establish procedures to access, gather, integrate, and provide for reporting of relevant and credible information across the NCDHHS enterprise (including but not limited to human resources physical security, information assurance, risk, and legal review); deter employees from becoming Insider threats; detect Insiders who pose a risk to information; and mitigate the risk of Insider threats while meeting privacy requirements and expectations.

2. Shall establish user activity monitoring using existing monitoring capabilities but with enhanced toolsets to baseline and detect activity indicative of Insider threat behavior on systems.

3. Shall establish a system or process to identify patterns of unauthorized disclosure or misuse in handling critical assets and information, even for incidents that do not warrant a culpability or incident report.

4. Shall oversee the collection, analysis, and reporting of information across NCDHHS to support the identification and assessment of Insider threats.

5. Shall upon detection of a security incident, coordinate with the Incident Response Team to follow the Enterprise Incident Response Procedure and Business Unit Protocols.

6. Shall conduct self-inspections of the ITP on a continuing basis, including the self-inspection related to the activity, information, information systems, and conditions of the overall security program, to include the ITP; have sufficient scope, depth, and frequency; and management support in execution and remedy.

7. Shall provide Insider Threat training for ITP personnel and awareness for in-scope employees.

8. Shall establish and manage all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to Senior Management.

Key Definitions for this Policy

Advanced Persistent Industry Threats: A sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged period.

Confidential Data: Department data that if exposed may cause financial and/or reputational impact to the department.

Data Manipulation: Occurs when a malicious actor alters, adjusts, or modifies the valuable digital documents and critical data instead of immediately stealing the data to damage the organization or cause disruption.

Data Theft: The act of stealing information from an unknowing victim with the intent of compromising privacy or obtaining confidential information.

Emerging Threats: Newly created or noticed and growing in strength or popularity: becoming widely known or established.

Espionage: The act of spying or secretly watching a person, department, government, etc., for the purpose of gathering protected information or detecting wrongdoing, and to transfer such information to another organization or state.

Insider Threat: The likelihood, risk, or potential that an employee, contractor, or vendor will use his or her authorized access, wittingly or unwittingly to do harm to the security of NCDHHS.

Internal Data: Department data used day-to-day that might not cause damage to NCDHHS but should be kept private.

Public Data: Department data that may cause minimal harm to NCDHHS because this data is publicly shared or available.

Reputational Damage: An act to cause harm to the organization's trust with the employees or the public.

Restricted Data: Sensitive information intended for use strictly within a limited group of NCDHHS employees.

Sabotage: To damage or destroy equipment or buildings to prevent the success of an individual or organization.

Unintentional Data Leak: Inadvertently places sensitive information or data in a location that is easily accessible by others without authorized access.

Exceptions:

No exceptions at this time.