INSIDER RISK PROGRAMS for the Healthcare and Public Health Sector

IMPLEMENTATION GUIDE

As a member of the Healthcare and Public Health Sector, you play a significant role in national security by protecting the Nation and its economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters.

Trusted insiders, both witting and unwitting, can cause grave harm to your organization's facilities, resources, information, and personnel. Insider incidents account for billions of dollars annually in "actual" and "potential" damages and lost revenue related to data breaches, trade secret theft, fraud, sabotage, damage to an organization's reputation, acts of workplace violence, and more.

Implementation of an Insider Risk Program can help mitigate risks associated with trusted insiders. Click the links to learn how to establish an Insider Risk Program at your organization and develop a risk management strategy that addresses areas critical to healthcare and public health.

Understanding Insider Risks

Establishing an Insider Risk Program

Insider Risk Management Strategy

Insider Risk Program Resources

UNDERSTANDING INSIDER RISK

Insider Risk Programs for the Healthcare and Public Health Sector—Implementation Guide

WHAT IS INSIDER RISK?

Anyone with authorized access who uses that access to wittingly or unwittingly harm the organization or its resources. Insiders can include employees, vendors, partners, suppliers and others that you provide access to your facilities and/or information. Most insider threats exhibit risky behavior prior to committing negative workplace events. If identified early, many risks can be mitigated before harm to the organization occurs. Learn more about insider risk indicators and find free training and awareness materials here.

WHAT RISKS DO INSIDERS POSE TO HEALTHCARE AND PUBLIC HEALTH?

Numerous threats have the potential to cause major disruption in healthcare and public health operations. These include malicious acts committed by insiders such as fraud, theft, sabotage, workplace violence, and more. Unwitting insiders may inadvertently disclose protected health information or other Health Insurance Portability and Accountability Act protected data, proprietary or other sensitive information, and unknowingly download malware or facilitate other cybersecurity events. The healthcare and public health sector is also vulnerable to supply chain failures, contamination, and threats to industrial control systems or other technical systems. Unmitigated insider risk is likely to increase these vulnerabilities. Click ____ to learn about real world insider incidents in the healthcare and public health sector.

WHY ESTABLISH AN INSIDER RISK PROGRAM?

Insider Risk Programs detect, deter, and mitigate the risks associated with trusted insiders. Multidisciplinary teams or "hubs" comprised of security, human resources, cyber, legal and other professionals from throughout your organization gather, integrate, and assess information indicative of potential risk and determine appropriate mitigation response options on a case by case basis. Most of these responses allow individuals to retain their position and receive assistance while protecting the organization and its assets. Insider Risk programs also protect the privacy of the workforce while reducing potential harm to the organization. See the Establishing an Insider Risk Program section to learn more.

WHAT CAN MY ORGANIZATION DO TO MINIMIZE THE RISKS ASSOCIATED WITH TRUSTED INSIDERS?

Effective Insider Risk programs deploy risk management strategies that identify the assets or resources to be protected, identify potential threats, determine vulnerabilities, assess risk, and deploy countermeasures. Many countermeasures are no or low cost to the organization and include training and awareness, clear reporting policies, managing organizational trust, and enhanced security procedures. Review the Insider Risk Management Strategy to learn more.

WHAT RESOURCES ARE AVAILABLE TO ME?

The Defense Counterintelligence and Security Agency, Department of Homeland Security, National Insider Threat Task Force, Federal Bureau of Investigation, and the

59% of Healthcare Data Breaches are from Insiders

The Verizon 2019 Data Breach Investigations Report (DBIR May 8 2019) is built upon analysis of 41,686 security incidents, of which 2,013 were confirmed data breaches. Of those breaches in the healthcare industry, 59% involved insiders. Another 4% involved partners given authorized access. 83% were financially motivated. Additional motivations included "fun," convenience, grudges, and espionage. 72% compromised medical data, 34% personal data, and 25% involved credentials used to access systems, applications, or databases.

Return to Main Page

ESTABLISHING AN INSIDER RISK PROGRAM

Insider Risk Programs for the Healthcare and Public Health Sector—Implementation Guide

SETTING UP YOUR PROGRAM

- **An Insider Risk Program is a multi-disciplinary activity or "hub"** established by an organization to gather, monitor, and assess information for insider risk detection and mitigation. Program personnel analyze information and activity indicative of insider risk and determine appropriate mitigation response options up to and including referral to the appropriate officials for investigation and/or resolution. Best practices encourage the Insider Risk Program to include a multidisciplinary team consisting of Legal Counsel, Security, Counterintelligence, Cybersecurity, Mental Health and Behavioral Science, and Human Resources or Human Capital disciplines. The ex- act makeup of your insider risk program will depend on the size and complexity of your organization.
- Insider Risk Programs take proactive measures to **deter, detect, mitigate, and report the threats** associated with trusted insiders. The program identifies anomalous behaviors that may indicate an individual poses a risk. Early identification allows Insider Risk program personnel to focus on an individual's issues of concern or stressors and deploy appropriate mitigation responses. When necessary, the team shares relevant information from each discipline with organizational leadership to facilitate timely, informed decision-making and reports information outside the organization as required.
- The first step in establishing your program is to **identify the program office and leadership**. You must determine how the team will be structured and where it will be located. Does your organization have the ability to house the team in a single location? Or, are the team members geographically separated and must rely on virtual communications to conduct operations? Your organization should select an Insider Risk program Senior Leader or Program Manager that oversees day-to-day operations. They will work with the organization's senior leadership to determine resource and staffing needs.
- You should **establish rules for how the Insider Risk program will operate** within your organization. As part of rule and policy development, the Insider Risk program should also identify practices for safeguarding sensitive personnel information along with consequences for violations of internal rules committed by Insider Risk program team members. Insider Risk team members must maintain standards of professional conduct like any other personnel. However, because you're dealing with extremely sensitive information, it's important that you clarify these responsibilities up front. A sample Insider Risk Program Plan is included in the Resources section.
- You should also **ensure that Insider Risk Program personnel are properly trained** to conduct their duties. Insider Risk program personnel must be able to appropriately respond to incident reporting, protect privacy and civil liberties, support mitigation options, and refer matters as required. Many free training options exist. Consult the Resources section for more information.

Return to Main Page

DETECTING AND DETERRING INSIDER THREATS

- The purpose of an Insider Risk program is to proactively deter, detect, mitigate, and report threats associated with trusted insiders. These actions make up your daily operations. Insider Risk Programs detect individuals at risk of becoming insider threats by identifying potential risk indicators. These observable and reportable behaviors or activities may indicate an individual is at greater risk of becoming a threat. Insider Risk Hubs deter potential insider threats by instituting appropriate security countermeasures, including awareness programs.

- **Training and Awareness Programs.** You must train and exercise your workforce to recognize and report potential risk indicators. It is a best practice to require personnel to complete initial and annual Insider Risk Awareness training. You can also maintain workforce awareness of insider risks and employee reporting responsibilities year round by instituting a vigilance campaign. Insider Risk programs can also conduct internal evaluations. These are small exercises used to test your workforce's knowledge of insider risk indicators and reporting requirements. These exercises do not have to be elaborate but should help you gauge the effectiveness of your program. You may use information from these evaluations to adjust your training and awareness program to ensure effectiveness. See the Resources section for access to free training and awareness materials.

- **Reporting Procedures.** Your Insider Risk Program must establish reporting procedures for the general workforce. Those that witness potential indicators should know exactly, when, where, and how they can report the information. Prepare procedures for "walk-ins" or those that may want to report their information face to face. Procedures should also include hotlines or dedicated email addresses. Individuals should be encouraged to self-report any issues they may be experiencing. One of the goals of an Insider Risk Program is to deter adverse actions by pointing those asking for assistance to resources that can help them. The challenge is to have people see the Insider Risk program as a resource rather than a punitive element. You can build this rapport by informing the workforce of your program, the mission, and its goals; by respecting privacy and civil liberties, and by deploying appropriate insider risk mitigation responses.

- **Organizational Justice.** As a best practice, Insider Risk Programs should consider the concept of organizational justice. Organizational justice refers to employee perceptions of fairness in the workplace. Labor relations can have an overall effect on the number of insider threat incidents you see. The worse the labor relations are, the more incidents you may encounter. Counterproductive workplace environments have consequences that can lead to disgruntlement. Organizational leadership that develops a positive workplace environment keeps the workforce engaged and productive. This same concept applies to the Insider Risk program. Ensuring appropriate mitigation response options and the protection of privacy and civil liberties in the conduct of your duties will minimize negative outcomes from maladaptive responses. Being responsive to workforce concerns is a great way to build rapport with personnel, encourage future reporting, and mitigate risk.

Return to Main Page

INSTITUTING USER ACTIVITY MONITORING

- **User Activity Monitoring (UAM) is the technical capability to observe and record the actions and activities of an individual operating on your computer networks** in order to detect potential risk indicators and to support mitigation responses. Logging, monitoring, and auditing of information system activities can lead to early discovery and mitigation of behavior indicative of insider threat. UAM also plays a key role in prevention, assistance, and response to acts of violence. As such, UAM development should include consideration of potential acts of violence against organizational resources, including suicidal ideation.

- Implementation will be specific to your location, but as a best practice, your organizations should:
  - ◊ Define what will be monitored
  - ◊ Indicate how monitoring will be instituted
  - ◊ Inform users of monitoring actions via banners
  - ◊ Identify indicators that require review (e.g., trigger words, activities)
  - ◊ Protect user activity monitoring methods and results
  - ◊ Develop a process for verification and review of potential issues
  - ◊ Establish referral and reporting procedures
- **Establishing baseline user behaviors** will make deviations or anomalies stand out from normal activities. It will also help determine what your user activity monitoring triggers, also known as internal security controls, should be. Once a "Normal Activity" baseline is established, internal security controls help us identify deviations. For example, user activity monitoring could help identify a rash of IT system misuses that suggest an employee needs some retraining. Another example would be access control logs indicating an employee is working irregular hours or has unexplained absences from work. User Activity Monitoring can help identify potential risk indicators that can be evaluated during your risk management and mitigation process.
- For more information, access the Insider Threat Indicators in User Activity Monitoring job aid.
- Now that you've established an Insider Risk program, it's time to employ risk management and mitigation strategies. Your Insider Risk Program should be able to identify and mitigate many issues before they escalate into negative behavior and respond appropriately when preventative actions are not feasible. Access the **Insider Risk Management Strategy** section to learn more.

Return to Main Page

Risk Analysis

Risk based analysis allows the Insider Risk Program to manage risk in a complex threat environment. The process of identifying assets, assessing threats and vulnerabilities, evaluating risk, and identifying countermeasures can help **determine the risks most closely associated with trusted insiders in the healthcare and public health sector** and the best methods to deter and mitigate them. It also allows your organization to differentiate between demanding threats to your enterprise and less pressing matters.

Identify Critical Assets

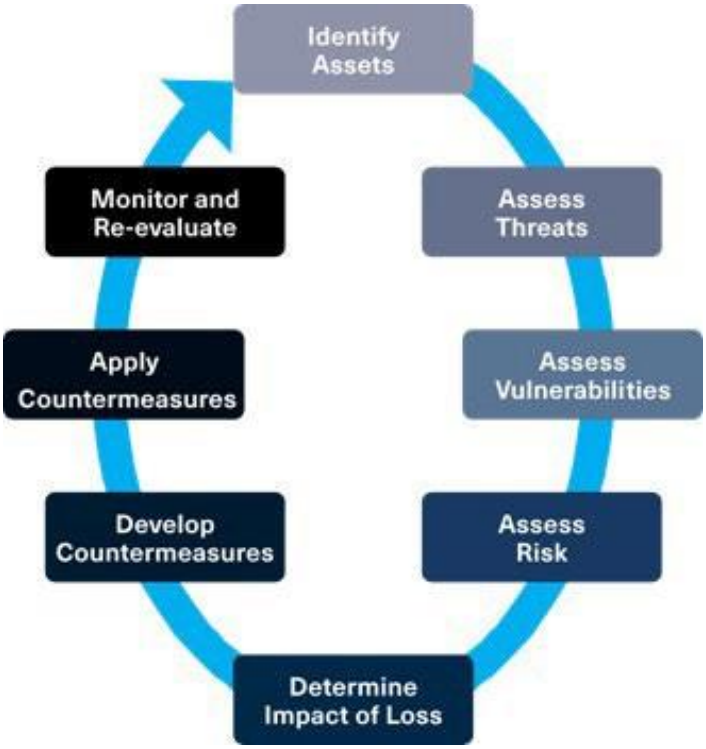
- The most basic function of an Insider Risk program is to protect the assets that are required by law and policy (such as HIPAA data) and/or that provide your organization with a competitive advantage (such as proprietary data, sensitive information, or processes). A critical asset is something of value that which if destroyed, altered, or otherwise de-graded would impact confidentiality, integrity, or availability and have a severe negative affect on the ability for the organization to support essential missions and business functions.
- **Critical assets can be both physical and logical** and can include facilities, systems, equipment, and technology. An often-overlooked aspect of critical assets is intellectual property. This may include proprietary software, customer data for vendors, schematics, and internal lab or other medical development processes. The organization must keep a close watch on where data is at rest and in transport. Current technology allows more seamless collaboration than ever, but also allows the organization's sensitive information to be easily removed from the organization.
- A complete understanding of critical assets (both physical and logical) is invaluable in defending against attackers who will often target the organization's critical assets. The following questions help the organization to identify and prioritize the protection of its critical assets:
    - ◊ What critical assets do we have?
    - ◊ Do we know the current state of each critical asset?
    - ◊ Do we understand the importance of each critical asset and explain why it is critical to our organization?
    - ◊ Can we prioritize our list of critical assets?
    - ◊ Do we have the authority, money, and resources to monitor our critical assets?
- The role of the Program Manager is to work across all areas of the organization to answer the questions above. Once those questions are answered within each division, input from senior level management should be obtained to prioritize protection across the organization. Once critical assets are identified and prioritized, the organization must **identify those high-risk users who most often interact with the critical systems or data**. This will help the organization to identify the best approaches to identify potential insider risks.

Return to Main Page

Conducting a Risk Assessment

The Risk Management Process
Risk management is a five-step process that provides a framework for collecting and evaluating information to:

- Identify assets (identify value of asset)
- Assess threats (intent and capability of adversaries)
- Assess vulnerabilities (identification and extent of vulnerabilities)
- Assess risk (determine the likelihood that a threat will exploit your vulnerabilities)
- Determine impact of loss, damage, or compromise of asset
- Develop countermeasures (security countermeasure options that can reduce or mitigate risks cost effectively)
- Apply countermeasures
- Monitor and re-evaluate



For More Information on Risk Management, click here

- Once you have identified critical assets, work to assess and analyze threats to, vulnerabilities of, and consequences of, disruption to your organization.
- Ensure that your assessment considers the physical, cyber, and human elements of security and resilience, supply chain issues, and your interdependence on vendors, partners, and other critical infrastructure sectors.
- Translate your analysis into actionable countermeasures that can be deployed to reduce or mitigate risks and inform response and recovery actions.
- Consult the Healthcare and Public Health Sector-Specific Plan issued by the Department of Homeland Security -CISA
- You may also consider implementing the Risk Management Framework (RMF) for information systems. More information on RMF is available from the National Institute of Standards and Technology. You can also access free training on the topic here.

Return to Main Page

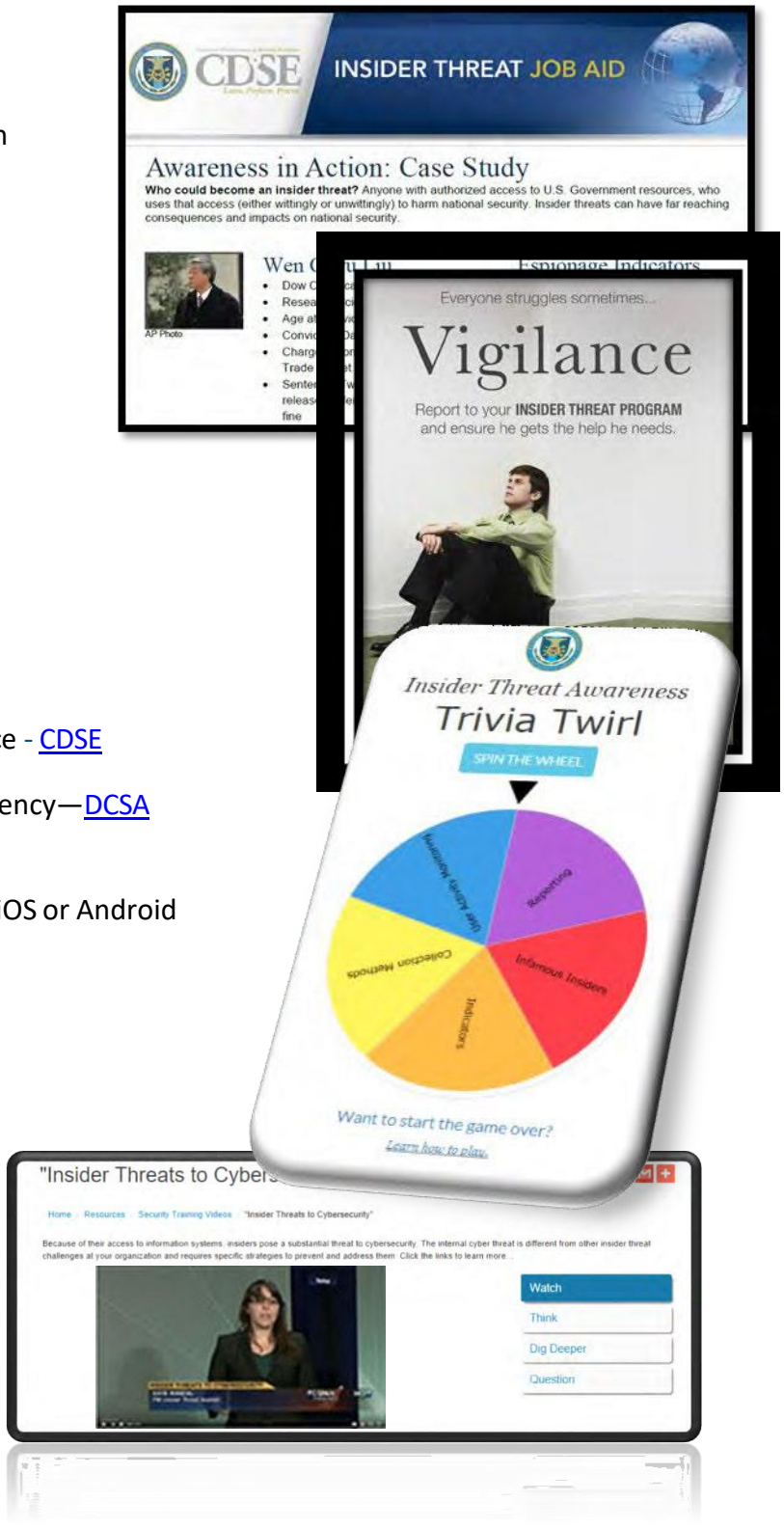
Risk Mitigation

- To be effective, Insider Risk programs must be on the lookout for potential issues before they pose a threat. In most cases, **proactive mitigation responses provide positive outcomes for both the organization and the individual.** This allows you to protect information, facilities, and personnel, retain valuable employees, and offers intervention to help alleviate the individual's stressors.
- Your Insider Risk Program's responses are situationally dependent, but may include recommendations such as:
    - ◊ Suspending access to information
    - ◊ Taking personnel actions such as counseling, referral, or termination
    - ◊ Organizational responses that may require changes to policy or procedures
    - ◊ Increased or additional training
- Human Resources Insider Risk Program team members can assist with counseling referrals or prescribed human resource interventions which may be corrective in nature. They deal with Employee Assistance Programs for resources in financial counseling, lending programs, mental health, and other well-being programs.
- Insider Risk Program team members from the various security disciplines, whether cyber, personnel, information, or physical, can assist with mitigation response options such as updating security protocols, adjusting UAM or other inspections, and providing basic security training and awareness to the workforce. **Some insider threat incidents may warrant external referrals to counterintelligence or law enforcement authorities**. Have a plan in place for referring these actions and consult with your legal counsel to ensure that proper protocols are followed.
- Your Program should **create a record of the incident outcome**. You may also create or coordinate with other elements within your organization to develop a "Damage Assessment" or "After Acton Report" that explains the damage to the organization, personnel, facilities, or other resources. You may need to work with the legal team and any other contributing elements to ensure the report is stored and retained appropriately. A sample Memorandum of Action Report is included in the Resources section.

Return to Main Page

INSIDER RISK PROGRAM RESOURCES

- **Sample Forms**
  - Insider RIsk Program Plan
  - Insider Risk Program Memorandum of Action
- **Training for Insider Risk Programs**
  - CDSE
  - DHS
- **Awareness Materials**
- **Case Studies**
- **Policies and Best Practices**
- **Supporting Organizations**
  - Department of Homeland Security—DHS
  - National Insider Threat Task Force—NITTF
  - Center for Development of Security Excellence - CDSE
  - Defense Counterintelligence and Security Agency—DCSA
  - Federal Bureau of Investigation—FBI
  - Insider Threat Sentry mobile application for iOS or Android on Apple App Store or Google Play
- **Insider Threat Body of Knowledge**



Return to Main Page

Case Study— DDoS attack at a medical facility via HVAC

A hospital facility employed the insider, a contractor, as a security guard. The insider was extensively involved with the Internet Underground and was the leader of a hacking group. The insider worked for the victim organization only at night and was unsupervised. The majority of the insider's unauthorized activities involved a heating, ventilation, and air conditioning (HVAC) computer. This HVAC computer was located in a locked room, but the insider used his security key to obtain physical access to the computer. The insider remotely accessed the HVAC computer five times over a two-day period. In addition, the insider accessed a nurses' station computer, which was connected to all of the victim organization's computers, stored medical records, and patient billing information.

The insider used various methods to attack the organization, including password-cracking programs and a botnet. The insider's malicious activities caused the HVAC system to become unstable, which eventually led to a one-hour outage. The insider and elements of the Internet Underground were planning to use the organization's computer systems to conduct a distributed-denial-of-service (DDoS) attack against an unknown target. A security researcher discovered the insider's online activities. The insider was convicted, ordered to pay $31,000 in restitution, and sentenced to nine years and two months of imprisonment followed by three years of supervised release.

This case illustrates how a single computer system can cause a great amount of damage to an organization. In this case, the damage could have been life threatening because the attack took place at a hospital facility. Modifying the HVAC system controls and altering the organization's environment could have affected temperature-sensitive drugs, supplies, and patients who were susceptible to temperature changes. With additional steps to bypass security, the insider could have potentially modified and impaired patient records, affecting treatment, diagnoses, and care. It is critical that management and information security teams work with other departments within an organization to identify critical systems. In this case, the HVAC computer was located in a locked room, not a data center or server room, which would have afforded the system additional protections and may have prevented the insider from manipulating the system.

In addition, the insider was able to access a nurses' station computer, which had access to other critical organizational systems. If the organization had fully understood the potential impact a compromised workstation could have on other parts of the organization, it could have implemented additional layers of protection that would have prevented this type of attack.

Return to Main Page

Case Studies— Insider Risk in the Healthcare Industry

A former worker at a New York City-based hospital, was convicted of crimes related to stealing patient information. Those included the theft of identity information from recently deceased patients, which he allegedly passed on to his wife. She pleaded guilty to charges related to using the stolen ID information of 80 emergency room patients to take over victims' credit card accounts and place fraudulent phone orders for designer merchandise valued at hundreds of thousands of dollars. She was convicted of several charges, including grand larceny, ID theft, and criminal possession of stolen property.

In another case, a doctor and former owner of several Texas hospitals who lost an appeal was resentenced to 135 months in federal prison for conspiracy to commit healthcare fraud, healthcare fraud, and aggravated identity theft. Federal prosecutors say that for more than three years, the doctor and others carried out a scheme to defraud Medicare and Medicaid through the submission of false claims. Prosecutors say the doctor and co-conspirators added, changed, and incorrectly sequenced diagnostic codes in a way that did not reflect the actual diagnoses and conditions of the patients. The false claims were submitted to Medicare and Medicaid for payment.

In a third case, New York prosecutors say four nursing home aides were recently charged with felonies and misdemeanors related to their alleged use of a smartphone to take "degrading" still and video images of residents at two facilities in Oswego, N.Y. Prosecutors note in a statement that both nursing homes say they have "strict policies" forbidding the use of cell phones by staffers and the creation of either still or video images of nursing home residents.

Access more Insider Risk case studies.

Return to Main Page

Sample Insider Risk Program Plan for _____

1. Purpose. This plan establishes policy and assigns responsibilities for the Insider Risk Program (IRP). The IRP will seek to establish a secure operating environment for personnel, facilities, information, equipment, networks, or systems from insider threats. An insider threat is defined as the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to an organization and its resources. Insider threats may include harm to the organizations information, personnel and facilities.

The program will gather, integrate, and report relevant and credible information indicative of potential insider risk indicators; deter insider threats; and detect risks posed by those with authorized access to any organizational resources to include personnel, facilities, information, equipment, networks, or systems. The program will proactively mitigate the risk of an insider threat as defined above.

2. Scope and applicability. This IRP applies to all staff offices, regions, and personnel with access to any organizational resources to include personnel, facilities, information, equipment, networks, or systems.

3. Guiding Principles.

a. _____ is subject to insider threats and will take actions to mitigate or eliminate those threats.

b. _____ will continually identify and assess risk to the organization and its personnel and institute programs to mitigate the risk.

4. Policy.

a. The IRP will protect personnel, facilities, and automated systems from insider risks. This program will seek to prevent theft, fraud, sabotage, acts of violence, and the loss of intellectual property, proprietary information, or other sensitive information. The program will actively deter trusted insiders from becoming insider threats. The program will establish the capability to detect insiders who pose a risk to information systems and information. The program will mitigate risks to the organization through administrative actions, referrals to law enforcement as appropriate, or other responses.

b. The IRP will follow identified best practices for insider risk programs and abide by the laws, policies, and regulations of local, state, and federal governments as appropriate.

c. The responsibilities outlined below enable the IRP to gather, integrate, centrally analyze, and respond appropriately to key threat-related information. The IRP will consult with records management and legal counsel to ensure any legal, privacy, civil rights, and civil liberties issues (including, but not limited to, the use of personally identifiable information) are appropriately addressed.

5. Responsibilities.

a. Insider Risk Program Senior Official (IRPSO) will be designated in writing and will act as the company's representative for IRP implementing activities.

b. The IRPSO will be responsible for daily operations, management, and ensuring compliance with the organizational policy.

c. Establish an Insider Risk Program based on the organization's size and operations.

d. Provide Insider Risk training for Insider Risk Program personnel and awareness training for the general workforce.

e. Establish user activity monitoring in order to detect activity indicative of insider threat behavior.

f. Establish procedures to access, gather, integrate, and provide for reporting of relevant and credible information across the organization (e.g., human resources, security, information assurance, and legal review) indicative of potential or actual insider risk to deter insider threats; detecting insider threats; and mitigate the risk of an insider threat.

g. Oversee the collection, analysis, and reporting of information across the organization to support the identification and assessment of insider threats.

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

_____ _____

Administrator Signature Date

This plan is a sample only and must be tailored to the specific Insider Risk Program procedures and processes in place at your organization.

Insider Risk Program Memorandum of Activity

Inquiry Number:	Reporting Date:	Source of Information:
Dates of Activity:	Date Report Drafted:	Location of Activity:
Type of Activity:	Subject of Inquiry:	Signature:

***ACTION**: Insider Risk program manager (Name) _____received a report from (Name of reporter) _____regarding (Name of subject) _____.*

The report was made to the Insider Risk Program based on the following:

The Insider Risk Program will take the following actions:

Coordinate/assess this referral with the Insider Risk Hub team.

***OUTCOME/NEXT STEPS**:*

Inquiry Number:	Reporting Date:	Source of Information:
Dates of Activity:	Date Report Drafted:	Location of Activity:
Type of Activity:	Subject of Inquiry:	Signature:

ACTION:

OUTCOME/NEXT STEPS:

Inquiry Number:	Reporting Date:	Source of Information:
Dates of Activity:	Date Report Drafted:	Location of Activity:
Type of Activity:	Subject of Inquiry:	Signature:

ACTION:

OUTCOME/NEXT STEPS:

Inquiry Number:	Reporting Date:	Source of Information:
Dates of Activity:	Date Report Drafted:	Location of Activity:
Type of Activity:	Subject of Inquiry:	Signature:

ACTION:

FINAL DISPOSITION:

No further action required _____.