Sample Incident Response Plan Erik Vargas

Incident Life Cycle

1. Preparation
   - Establish incident response roles and responsibilities (Responsible: Incident Response Team)
     - Incident Commander (Accountable)
     - Technical Team Lead (Responsible)
     - Communication Lead (Responsible)
     - Evidence Lead (Responsible)
     - Logistics Lead (Responsible)
   - Develop incident response procedures and guidelines (Responsible: Incident Response Team)
   - Conduct incident response training and exercises (Responsible: Incident Response Team)
   - Identify and document critical systems and data (Consulted: Technical Team Lead, Evidence Lead)
2. Detection and Analysis
   - Establish monitoring and detection capabilities to identify potential incidents (Responsible: Technical Team Lead)
   - Conduct a preliminary analysis to determine the nature and scope of the incident (Responsible: Technical Team Lead)
   - Notify the incident response team and relevant stakeholders (Informed: All relevant stakeholders)
3. Containment, Eradication, and Recovery
   - Contain the incident to prevent further damage (Responsible: Technical Team Lead)
   - Eradicate the cause of the incident (Responsible: Technical Team Lead)
   - Restore normal system operations (Responsible: Technical Team Lead)
   - Perform a post-incident review to identify areas for improvement (Consulted: All members of the Incident Response Team)
4. Post-Incident Activity
   - Conduct a debrief to review the incident response process and identify areas for improvement (Responsible: Incident Response Team)
   - Document the incident and the steps taken to resolve it (Responsible: Evidence Lead)
   - Update incident response procedures and guidelines based on lessons learned (Responsible: Incident Response Team)

    - Provide appropriate follow-up and reporting to stakeholders (Informed: All relevant stakeholders)

Incident Communication Channels

- Internal Communication Channels:
  (This can include email, intranet, internal instant messaging systems, and phone calls to reach all relevant personnel within the organization.)

- External Communication Channels:
  (This can include email, extranet, web portals, or phone calls to reach stakeholders outside the organization, such as customers, partners, or suppliers.)

- Emergency Notification Systems:
  (This can include automated voice or text messaging systems, or manual systems like sirens, that can be used to alert personnel of an incident in progress.)

- Media Outlets:
  (This can include traditional media like newspapers or television, as well as social media platforms.)

Measuring Effectiveness and Continuous Improvement of the Incident Response Plan

1. Exercise and Testing:
   Regularly conducting tabletop exercises, drills, and simulations can help identify gaps in the incident response plan and provide opportunities for improvement.

2. Post-Incident Reviews:
   Conducting a review of each incident, including the response and resolution process, can help identify areas for improvement and inform changes to the incident response plan.

3. Metrics and Key Performance Indicators (KPIs):
   Measuring key metrics, such as the time to detect an incident, the time to contain an incident, and the time to recover from an incident, can provide insight into the effectiveness of the incident response plan.

4. Feedback and Surveys:
   Gathering feedback and conducting surveys of those involved in the incident response process can provide valuable insight into areas where the incident response plan was effective and areas where improvements can be made.

5. Continual Improvement:
   Regularly reviewing and updating the incident response plan based on lessons learned from exercises, post-incident reviews, and feedback can help ensure the plan remains effective over time.