**Example of an incident management plan for an EKS cluster on AWS:**

**1. Incident Identification and Escalation:**

* Establish clear channels of communication and define primary and secondary points of contact for incident reporting.
* Monitor the EKS cluster using appropriate monitoring tools and establish alerting mechanisms for critical events or failures.
* When an incident is identified, it should be reported immediately to the designated incident response team.

**2. Initial Response:**

* The incident response team should gather all relevant information about the incident, such as symptoms, error messages, affected components, and any recent changes made to the cluster.
* Assess the severity and impact of the incident based on predefined criteria.
* Activate the appropriate incident response procedures based on the severity level.

**3. Incident Mitigation:**

* Based on the severity of the incident, perform initial steps to mitigate the issue.
* Follow established troubleshooting procedures to identify the root cause of the problem.
* Implement temporary workarounds or fixes if available to restore services or prevent further impact.

**4. Communication and Collaboration:**

* Maintain constant communication with stakeholders, including development teams, operations teams, and management, to provide regular updates on the incident status.
* Share incident details, impact, and progress towards resolution, adhering to established communication channels and guidelines.
* Collaborate with relevant teams, such as AWS support or third-party vendors, to leverage their expertise and assistance if necessary.

**5. Resolution and Recovery:**

* Implement permanent fixes or remediation steps to resolve the incident and prevent its recurrence.
* Perform necessary tests and validation to ensure the stability and integrity of the EKS cluster.
* Restore services to normal operation and verify that all affected components are functioning as expected.

**6. Post-Incident Review:**

* Conduct a post-incident review to analyze the incident response process and identify areas for improvement.
* Document lessons learned, including the root cause, actions taken, and any recommendations for future incidents.
* Update the incident management plan based on the findings and implement any necessary changes or improvements.

Remember, this is just an example, and the incident management plan should be tailored to your specific organization's needs and the characteristics of your EKS cluster.