Incidence Response playbook: Policy Violation

Phase 1: Incident Identification and Reporting

- Define what constitutes a policy violation in your organization. Examples could include unauthorized access to sensitive data, use of prohibited software or hardware, violation of acceptable use policies, or breach of data privacy rules.
- Establish clear channels for incident identification and reporting. This could include a designated email address, hotline, or incident reporting system.
- Clearly outline the roles and responsibilities of team members involved in incident response, including the incident response team (IRT), IT security team, legal team, and human resources team.

Phase 2: Initial Assessment and Triage

- When a potential policy violation is identified, the IRT should conduct an initial assessment to determine the severity and impact of the incident.
- Follow predefined procedures for triaging incidents based on severity levels. For example, a low-severity incident may require a different level of response compared to a high-severity incident.
- Determine if the incident is a false positive or a confirmed policy violation. This may involve verifying information, interviewing employees involved, or reviewing logs and records.

Phase 3: Incident Containment and Mitigation

- Once a policy violation is confirmed, take immediate action to contain the incident and prevent further damage. This could involve disabling accounts, removing access privileges, or isolating affected systems from the network.
- Follow predefined procedures for mitigating the impact of the policy violation. This may include restoring backups, patching vulnerabilities, or removing malicious software.
- Communicate with relevant stakeholders, including management, legal, and HR, to keep them informed about the incident and the steps being taken to mitigate it.

Phase 4: Investigation and Root Cause Analysis

- Conduct a thorough investigation to determine the root cause of the policy violation. This may involve reviewing logs, analyzing system configurations, and interviewing employees involved.
- Document all findings and evidence collected during the investigation. This information may be used for legal or regulatory purposes.
- Identify any gaps or weaknesses in existing policies or controls that contributed to the policy violation and take steps to address them to prevent similar incidents in the future.

Phase 5: Remediation and Recovery

- Develop a plan to remediate the policy violation and restore normal operations. This may involve implementing new controls, providing additional training or awareness programs, or updating policies and procedures.

- Monitor the systems and networks to ensure that the policy violation has been fully remediated and that there are no lingering issues.
- Conduct post-incident reviews to evaluate the effectiveness of the incident response process and identify areas for improvement.

Phase 6: Reporting and Documentation

- Document all actions taken during the incident response process, including timelines, decisions made, and evidence collected.
- Prepare a final report summarizing the incident, the actions taken, and the lessons learned. This report may be used for internal reviews, regulatory compliance, or legal purposes.
- Review and update the incident response playbook based on the findings from the incident and the post-incident review to continually improve the organization's incident response capabilities.

Note: I will tailor this incident response playbooks to the specific needs and requirements of your organization. It's important to regularly review and update the playbook to reflect changes in policies, procedures, and technologies, and to ensure that your incident response team is well-prepared to effectively respond to policy violations and other security incidents.