Introduction: The following incident response policy outlines the steps to be taken in case of a cybersecurity incident. The policy is designed to ensure that the incident is contained, analyzed, and resolved in a timely and effective manner.

1. Incident Identification: All employees, contractors, and vendors must immediately report any suspected or actual security incident to the designated point of contact (POC) for cybersecurity incidents. The designated POC for cybersecurity incidents is responsible for coordinating the response to the incident.
2. Incident Categorization: Upon receiving a report of a suspected or actual security incident, the designated POC for cybersecurity incidents will categorize the incident based on its severity and potential impact. The categories are as follows:

* Level 1: Low severity incidents that have a minimal impact on the organization's operations or assets.
* Level 2: Moderate severity incidents that have a significant impact on the organization's operations or assets.
* Level 3: High severity incidents that have a severe impact on the organization's operations or assets.

1. Incident Response Team Activation: Depending on the severity and impact of the incident, the designated POC for cybersecurity incidents will activate the appropriate incident response team. The incident response teams are as follows:

* Level 1 Incident Response Team: Composed of the designated POC for cybersecurity incidents and one or more IT staff members.
* Level 2 Incident Response Team: Composed of members from IT, Legal, Public Relations, and other relevant departments.
* Level 3 Incident Response Team: Composed of senior executives, Legal, IT, Public Relations, and other relevant departments.

1. Incident Containment and Analysis: The incident response team will immediately take steps to contain the incident and prevent further damage. The team will also conduct a thorough analysis of the incident to determine the scope, cause, and extent of the damage. The analysis will include collecting evidence and identifying any compromised systems or data.
2. Incident Resolution: Based on the analysis, the incident response team will develop and implement a plan to resolve the incident. The plan will include steps to restore normal operations, recover lost data, and prevent similar incidents from occurring in the future.
3. Communication and Reporting: The designated POC for cybersecurity incidents will be responsible for communicating the incident and its resolution to the appropriate stakeholders, including senior executives, Legal, IT, Public Relations, and other relevant departments. The communication will include a summary of the incident, its impact, and the steps taken to resolve it. The designated POC for cybersecurity incidents will also be responsible for documenting the incident and the response in detail.
4. Incident Follow-Up and Lessons Learned: After the incident has been resolved, the designated POC for cybersecurity incidents will conduct a review to identify any areas for improvement and lessons learned. The review will include a post-incident analysis, a review of policies and procedures, and recommendations for future incident response efforts.

Conclusion: The incident response policy is designed to ensure that the organization can effectively respond to cybersecurity incidents in a timely and effective manner. By following the policy's guidelines, the organization can minimize the impact of an incident and prevent similar incidents from occurring in the future.