Objective: This template is designed to guide the students through the essential components of a comprehensive recovery plan in the event of a ransomware attack.

Recovery Plan Development Template

School Name: <<Enter School Name Here>>
Date: <<Enter Date Here>>

1. Initial Assessment:

- **Summary of the Incident:** Briefly describe the ransomware attack and its impact on the school's network and data.
- **Resources Affected:** List the systems, data, and services affected by the ransomware.

2. Immediate Response Actions Taken:

- **Containment Measures:** Outline the steps taken immediately after the attack was discovered to prevent further spread.
- **Communication Actions:** Detail how the incident was communicated internally and externally, and any liaisons with law enforcement or cybersecurity experts.

3. Recovery Strategy:

- **Data Restoration Plan:** Describe the approach to recover encrypted or lost data, including the use of backups.
- **System Restoration:** Outline the process for safely restoring systems and services to full functionality.
- **Timeline for Recovery:** Provide a realistic timeline for each step in the recovery process.

4. Security Enhancement Measures:

- **Vulnerability Rectification:** Identify the vulnerabilities exploited in the attack and propose measures to rectify them.
- **Future Prevention Strategies:** Suggest additional cybersecurity measures to prevent similar attacks in the future.
- **Training and Awareness Programs:** Recommend training initiatives for staff and students to enhance cybersecurity awareness.

5. Post-Recovery Analysis:

- **Lessons Learned:** Reflect on the incident and identify key lessons learned about cybersecurity and crisis management.
- **Future Plan Updates:** Discuss how this experience will inform updates to the school's cybersecurity policies and emergency response plans.

6. Additional Considerations:

- **Budget Implications:** Estimate the financial impact of the attack and the cost of implementing the recovery plan.
- **Legal and Compliance Issues:** Address any legal or regulatory implications arising from the attack and the school's response.

7. Approval and Implementation:

- **Approval Signatures:** Space for signatures from the designated authorities (e.g., school principal, IT department head).
- **Implementation Plan:** Outline the steps and timeline for implementing the recovery plan.