Developed a Plan to Disseminate and Evaluate Password Protected Policies

Dissemination Plan:

1. Communication Strategy:
   - Objective: Ensure a comprehensive understanding of the Password Protection Policy among all employees.
   - Approach:
     - Utilise a multi-channel communication approach, including email, training sessions, and internal communication platforms.
2. Training Sessions:
   - Objective: Educate employees on the importance of password protection and the specifics of the new policy.
   - Approach:
     - Conduct in-person or virtual training sessions led by cybersecurity experts.
     - Use engaging presentations, real-life examples, and interactive elements to enhance learning.
3. Training Materials:
   - Objective: Provide supporting materials for ongoing reference and reinforcement.
   - Approach:
     - Develop visually appealing infographics, presentations, and handouts.
     - Create an online training module accessible through the company's learning management system (LMS).
4. Email Communication:
   - Objective: Ensure all employees receive clear information about the new policy.
   - Approach:
     - Send a series of targeted emails with key policy points, links to the policy document, and training resources.
     - Use language that emphasises the benefits of strong password practices.
5. Intranet and Company Portals:
   - Objective: Provide easily accessible resources and information.
   - Approach:
     - Publish the Password Protection Policy prominently on the company intranet and employee portal.
     - Include FAQs, links to training materials, and relevant news articles.
6. Posters and Signage:
   - Objective: Reinforce key points visually in common areas.
   - Approach:
     - Design eye-catching posters and signage for display in break rooms, common areas, and near workstations.
     - Include visuals and slogans to grab attention.

7. Managerial Support:
   - Objective: Ensure buy-in and support from managers and team leaders.
   - Approach:
     - Engage managers to endorse the policy during team meetings.

    - Encourage managers to lead by example in implementing strong password practices.

8. Feedback Channels:
    - Objective: Establish open lines of communication for employee feedback and questions.
    - Approach:
        - Set up an email address or an anonymous feedback platform for employees to ask questions or express concerns.
        - Encourage an open dialogue to address any confusion or uncertainties.

Evaluation Plan:

1. Post-Training Assessments:
    - Objective: Measure the effectiveness of training sessions.
    - Approach:
        - Conduct post-training assessments or quizzes to gauge understanding.
        - Analyse results to identify areas that may need additional clarification.
2. Policy Acknowledgment:
    - Objective: Ensure employees acknowledge and understand the policy.
    - Approach:
        - Implement an electronic acknowledgment process requiring employees to confirm receipt and understanding of the policy.
3. Compliance Audits:
    - Objective: Assess adherence to the Password Protection Policy.
    - Approach:
        - Periodically conduct compliance audits to review password-related metrics, such as change frequency and complexity.
        - Identify and address non-compliance issues.
4. Security Awareness Metrics:
    - Objective: Track metrics related to overall security awareness.
    - Approach:
        - Monitor participation rates in training modules and simulated phishing exercises.
        - Evaluate improvements in awareness over time.
5. Employee Surveys:
    - Objective: Gather feedback on the clarity and effectiveness of the policy.
    - Approach:
        - Conduct anonymous surveys to assess employee perceptions of the Password Protection Policy.
        - Use survey results to refine training materials and communication strategies.

6. Continuous Improvement:
    - Objective: Enhance the policy based on feedback and evaluation results.
    - Approach:

        - Establish a process for continuous improvement, regularly updating the policy to address emerging threats.
        - Communicate changes effectively to employees.

7. Recognition and Rewards:
    - Objective: Encourage positive behaviour through recognition.
    - Approach:
        - Implement a recognition program for individuals or teams demonstrating exemplary adherence to the Password Protection Policy.
        - Use positive reinforcement to promote good security practices.
8. Communication Channels:
    - Objective: Maintain open channels for ongoing communication.
    - Approach:
        - Keep communication lines open for employees to report security concerns or seek clarification.
        - Address feedback promptly and transparently.
9. Annual Reviews:
    - Objective: Ensure the policy remains relevant and effective.
    - Approach:
        - Conduct annual reviews of the Password Protection Policy, considering changes in the organisational landscape and evolving security threats.
        - Update the policy as needed.