1. What is one key action a computer security professional should take to protect sensitive customer data?
2. A company stores customer personal data on an internal server. You discover that the server is not encrypted and is accessible to several unauthorized employees. Management asks you to ignore the issue for now because fixing it may disrupt operations. As a computer security professional, what are your legal and professional responsibilities in this situation, and what actions should you take to safeguard the data and mitigate potential risks?

3. Why are transparency and accountability important in computer security practice?

4. You are part of a security team that recently experienced a minor data breach affecting a small number of users. Your supervisor suggests not reporting the incident publicly to avoid damaging the organization’s reputation. How should professionalism, ethical conduct, transparency, and accountability guide your decision in this scenario? Explain the actions you would take and justify them.
5. Why is it important for a computer security professional to consider both ethical and legal factors before making a security-related decision?
6. While performing a security assessment, you discover a serious vulnerability in a system used by many external users. Reporting it immediately could cause public concern, but delaying disclosure increases the risk of exploitation. How would you apply informed judgment to decide when and how to disclose the vulnerability, considering legal, ethical, and professional responsibilities?