Detailed Rubric for Final Cybersecurity Project

---

1. Initial Analysis (20 points)

1.1 Identifying How the Breach Occurred (10 points)

Criteria	Points
Comprehensive identification of the breach method	
- Correctly identifies the exact method used by attackers (e.g., specific phishing email, exploited vulnerability)	**10**
- Identifies the general method but lacks specifics	**7**
- Partially identifies the method with inaccuracies	**4**
- Incorrect or no identification of the breach method	**0**

1.2 Assessing the Extent of the Damage (10 points)

Criteria	Points
Thorough assessment of affected data and systems	
- Accurately lists all compromised data types and systems	**10**
- Identifies most compromised data and systems with minor omissions	**7**
- Identifies some compromised data but misses key elements	**4**
- Fails to identify compromised data and systems	**0**

---

2. Designing Solutions (25 points)

2.1 Technical Measures (15 points)

Criteria	Points
Proposes effective technical solutions	
- Suggests at least three relevant technical measures (e.g., implementing advanced firewalls, encryption, multi-factor authentication) with detailed explanations	**15**
- Proposes two relevant technical measures with explanations	**10**
- Suggests one technical measure or provides vague solutions	**5**
- No technical solutions proposed	**0**

2.2 Non-Technical Solutions (10 points)

Criteria	Points
Recommends appropriate non-technical measures	
- Suggests at least two non-technical solutions (e.g., employee training programs, policy revisions) with detailed plans	**10**
- Proposes one non-technical solution with some detail	**5**
- Provides irrelevant or impractical solutions	**2**
- No non-technical solutions proposed	**0**

---

3. Ethical Dilemmas (15 points)

3.1 Discussion of Disclosure (7 points)

Criteria	Points
Analyzes whether to disclose the breach	
- Provides a well-reasoned argument for or against disclosure, referencing ethical principles and potential impacts	**7**
- Offers an opinion with limited reasoning	**4**
- Provides a superficial or unclear stance	**2**
- Does not address the disclosure issue	**0**

3.2 Evaluation of Stakeholder Interests (8 points)

Criteria	Points
Evaluates conflicts between stakeholders	
- Thoroughly discusses at least two stakeholder perspectives (e.g., customers, employees, shareholders) and potential conflicts	**8**
- Mentions one stakeholder perspective with some discussion	**4**
- Briefly notes stakeholder interests without depth	**2**
- Does not address stakeholder conflicts	**0**

---

4. Technical Implementation (25 points)

4.1 Encryption/Decryption Example (5 points)

Criteria	Points
Correct implementation of encryption/decryption	
- Accurately encrypts and decrypts provided plaintext using correct keys and methods	**5**
- Completes encryption or decryption with minor errors	**3**

- Attempts encryption/decryption but with major errors	**1**
- No attempt or incorrect methods used	**0**

4.2 Network Traffic Analysis (15 points)

Criteria	Points
Identifies suspicious activities in network logs	
- Correctly identifies all anomalies and explains their significance	**15**
- Identifies most anomalies with reasonable explanations	**10**
- Identifies some anomalies but misses key issues	**5**
- Fails to identify suspicious activities	**0**

4.3 Password Policy and Strength Testing (5 points)

Criteria	Points
Proposes a secure password policy and tests strength	
- Develops a comprehensive password policy and correctly uses tools to test password strength	**5**
- Provides a basic password policy with minimal testing	**3**
- Suggests weak policy or incorrect testing methods	**1**
- No policy proposed or testing performed	**0**

---

5. Presentation and Report (15 points)

5.1 Report Quality (10 points)

Criteria	Points
Clarity, organization, and completeness of the report	
- Report is well-organized, free of grammatical errors, and includes all required sections with detailed content	**10**
- Report is organized with minor errors and most sections included	**7**
- Report lacks organization, has multiple errors, or missing sections	**4**
- Report is poorly written and incomplete	**0**

5.2 Presentation Delivery and Visuals (5 points)

Criteria	Points
Effectiveness of presentation and use of visuals	
- Presentation is clear, engaging, within time limit, and uses effective	**5**

visuals (e.g., slides, diagrams)	
- Presentation is clear but slightly over time or visuals are basic	**3**
- Presentation lacks clarity, is disorganized, or visuals are poor	**1**
- No presentation delivered	**0**

Total Points: 100

Additional Notes:

- **Timeliness:** Late submissions may result in point deductions according to the course late policy.
- **Originality:** All work must be original. Plagiarism will result in a score of zero for the affected sections.
- **Collaboration:** While discussion with peers is allowed, the final work must be individual.

Summary Table

Below is a condensed table summarizing the point distribution:

Component	Criteria	Points
1. Initial Analysis	1.1 Identifying Breach Method	10
	1.2 Assessing Damage Extent	10
2. Designing Solutions	2.1 Technical Measures	15
	2.2 Non-Technical Measures	10
3. Ethical Dilemmas	3.1 Discussion of Disclosure	7
	3.2 Evaluation of Stakeholder Interests	8
4. Technical Implementation	4.1 Encryption/Decryption Example	5
	4.2 Network Traffic Analysis	15
	4.3 Password Policy and Strength Testing	5
5. Presentation and Report	5.1 Report Quality	10
	5.2 Presentation Delivery and Visuals	5
Total		**100**