Okay, I understand. I will revise the previously generated cybersecurity policy prompt, incorporating the provided feedback and suggestions to create a more robust, detailed, and actionable policy. I will pay particular attention to vulnerability management, third-party risk management, data retention schedule examples, DPO responsibilities, specific encryption protocols/standards, a legal review reminder, policy versioning, and clearly accessible incident reporting contact information.

Here's the revised prompt:

```
You are an expert cybersecurity policy writer. Your task is to generate a comprehensive cybersecurity policy for a hypothetical medium-sized enterprise (250-500 employees) called "Acme Corp," operating in the e-commerce sector and handling sensitive customer data, including payment information. Acme Corp. is based in the EU and is therefore subject to GDPR.

The policy should be written in clear, professional language suitable for distribution to all employees. It should be thorough, covering all essential aspects of cybersecurity, and providing actionable guidance. Assume that Acme Corp. has a dedicated IT department and a designated Data Protection Officer (DPO). The policy should include placeholders (indicated by "[LINK TO...]" or "[SPECIFIC EXAMPLE]") for linking to specific procedures, standards, or examples within Acme Corp.

The policy must explicitly address the following elements:

I. Introduction:

• Purpose and scope of the policy
• Commitment to cybersecurity
• Applicability to all employees, contractors, and third-party vendors

II. Definitions:

• Define key terms such as "Data Breach," "Personal Data," "Confidential Information," "Malware," "Phishing," etc. Provide concise and easily understandable definitions.

III. Data Protection Principles (GDPR Alignment):

• Lawfulness, Fairness, and Transparency: Data processing must have a legal basis (consent, contract, legal obligation, vital interests, public interest, legitimate interests). Specify the legal bases Acme Corp. relies upon for different types of data processing. Address fairness and transparency requirements, including providing clear information to data subjects.
• Purpose Limitation: Data can only be collected for specified, explicit, and legitimate purposes.
• Data Minimization: Only collect data that is adequate, relevant, and limited to what is necessary.
• Accuracy: Ensure data is accurate and kept up to date.
• Storage Limitation: Data will be retained only for as long as necessary. Refer to a data retention schedule. [LINK TO DATA RETENTION SCHEDULE]. Provide specific examples within
```

the policy to illustrate the application of the data retention schedule. For example:

- "Customer order information will be retained for seven (7) years for accounting and warranty purposes."
- "Employee personnel files will be retained for seven (7) years after termination of employment, as required by applicable employment law."
- "Website access logs will be retained for three (3) months for security and performance monitoring."
- Integrity and Confidentiality: Data must be processed securely, using appropriate technical and organizational measures.

IV. Roles and Responsibilities:

- Clearly define the roles and responsibilities of:
- Executive Management
- IT Department
- Data Protection Officer (DPO):
- Specifically outline the DPO's responsibilities, including: "Monitoring compliance with this policy and applicable data protection laws; Providing advice and guidance to the organization on data protection matters; Acting as the point of contact for data subjects and supervisory authorities; Conducting data protection impact assessments (DPIAs)." Provide the DPO's contact information: [DPO Contact Information: Name, Title, Email, Phone].
- All Employees

V. Data Security Controls:

- Access Control: Implement strong access controls to restrict access to sensitive data. Include principles of least privilege and need-to-know. [LINK TO ACCESS CONTROL POLICY]
- Authentication: Use strong passwords, multi-factor authentication (MFA), and other authentication mechanisms.
- Encryption: Encrypt sensitive data both in transit and at rest. Specify approved encryption protocols and standards (e.g., "Data in transit will be encrypted using TLS 1.3 or higher."; "Data at rest will be encrypted using AES-256 with GCM.").
- Data Loss Prevention (DLP): Implement DLP measures to prevent sensitive data from leaving the organization's control. [LINK TO DLP POLICY]
- Network Security: Firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation.
- Physical Security: Secure physical access to data centers and other sensitive areas.

VI. Incident Response:

- Establish a clear incident response plan for handling security incidents and data breaches. [LINK TO INCIDENT RESPONSE PLAN]
- Define roles and responsibilities during an incident.
- Outline procedures for reporting incidents. Provide clear and easily accessible contact information for reporting incidents (e.g., "Report all suspected security incidents immediately to the IT Security Team at [IT Security Team Email Address] or call the Security Hotline at [Security Hotline Phone Number]. After hours, contact [Designated

After-Hours Contact Information].").
- Include steps for investigation, containment, eradication, recovery, and post-incident analysis.
- Address data breach notification requirements under GDPR (including timelines).

VII. Vulnerability Management:

- Establish a process for identifying, assessing, and remediating vulnerabilities in systems and applications.
- Regular vulnerability scanning schedules.
- Patch management procedures (including timelines for applying patches). [LINK TO PATCH MANAGEMENT POLICY]
- Penetration testing (frequency and scope).

VIII. Third-Party Risk Management:

- Establish a process for assessing and managing the security risks associated with third-party vendors.
- Due diligence processes for selecting vendors (security questionnaires, audits of vendor security controls). [LINK TO THIRD-PARTY RISK ASSESSMENT PROCEDURE]
- Contractual requirements for data protection (Data Processing Agreements - DPAs).
- Ongoing monitoring of vendor security practices.
- Incident response plans for third-party breaches.

IX. Data Subject Rights (GDPR Alignment):

- Explain the rights of data subjects under GDPR:
- Right to access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling
- Provide clear instructions on how data subjects can exercise these rights. [LINK TO PROCEDURE FOR EXERCISING DATA SUBJECT RIGHTS]. This should include specific steps and contact information.

X. International Data Transfers:

- Outline the safeguards in place for transferring personal data outside the European Economic Area (EEA).
- Address the use of Standard Contractual Clauses (SCCs) / Data Processing Agreements (DPAs). [LINK TO DPA TEMPLATE]
- Describe the process for conducting Transfer Impact Assessments (TIAs). [LINK TO TIA PROCEDURE]
- Address reliance on adequacy decisions (if applicable).

XI. Security Awareness Training:

• Provide regular security awareness training to all employees.
• Training topics should include:
• Phishing awareness
• Password security
• Data protection principles
• Social engineering
• Malware prevention
• Safe internet browsing
• Incident reporting procedures
• Document training completion.

XII. Compliance and Enforcement:

• Outline the consequences of violating this policy.
• Regular audits and assessments to ensure compliance.
• Disciplinary actions for non-compliance. [LINK TO DISCIPLINARY POLICY]

XIII. Policy Review and Updates:

• This policy will be reviewed and updated at least annually, or more frequently as needed to reflect changes in business operations, legal requirements, or security threats.
• The [Designated Role/Committee] is responsible for reviewing and updating this policy.

XIV. Policy Versioning:

• Include a table at the beginning of the document to track policy versions and revision dates. Example:

Version	Date	Description of Changes	Author
1.0	2023-10-27	Initial Draft	[Name/Title]
1.1	2024-01-15	Added section on Vulnerability Management	[Name/Title]

Important Considerations:

• This policy should be reviewed and approved by legal counsel before implementation. [INCLUDE BOLDED STATEMENT: THIS POLICY SHOULD BE REVIEWED AND APPROVED BY LEGAL COUNSEL BEFORE IMPLEMENTATION.]
• Tailor the policy to the specific needs and risk profile of Acme Corp.
• Ensure that the policy is readily accessible to all employees.

By following this prompt, you will generate a comprehensive and actionable cybersecurity policy that will help Acme Corp. protect its data and comply with relevant regulations.
```
```