```python
def revise_cybersecurity_policy_prompt(policy_prompt):
"""
Revises the provided cybersecurity policy prompt based on the given feedback.

Args:
policy_prompt (str): The original cybersecurity policy prompt.

Returns:
str: The revised cybersecurity policy prompt.
"""

revised_prompt = """## Cybersecurity Policy for Healthcare Organizations

### 1. Introduction

This Cybersecurity Policy outlines the security standards and procedures that [Organization Name] will adhere to in order to protect the confidentiality, integrity, and availability of its information assets. This policy applies to all employees, contractors, vendors, and other authorized users who access or use [Organization Name]'s systems and data. As a healthcare organization operating in a medium-risk environment, we acknowledge the sensitive nature of Protected Health Information (PHI) and other confidential data we handle, and this policy is designed to mitigate associated risks while adhering to relevant compliance standards, specifically SOC 2, HIPAA, and other applicable regulations. The effectiveness of this policy relies on the participation and diligence of every member of our organization. This policy is aligned with SOC 2 Trust Services Criteria, specifically focusing on Security, Availability, Processing Integrity, Confidentiality, and Privacy, and details how controls are implemented and maintained to meet these criteria.

### 2. Risk Assessment

[Organization Name] will conduct regular risk assessments to identify, analyze, and prioritize cybersecurity risks. These assessments will cover all aspects of our information systems, including infrastructure, applications, and data.

- --Frequency:-- Risk assessments will be conducted at least annually, and more frequently when significant changes occur in our environment (e.g., new systems, regulations, or threats), or following a significant security incident.
- --Methodology:-- Assessments will employ a recognized risk management framework (e.g., NIST Cybersecurity Framework, ISO 27005, HITRUST CSF) and will consider both internal and external threats, vulnerabilities, and potential impacts. This includes both qualitative and quantitative analysis where appropriate.
- --Scope:-- The scope of risk assessments will include but not be limited to:
- Data security and privacy risks associated with PHI and other sensitive information.
- Risks related to third-party vendors and business associates.
- Technological vulnerabilities in systems and applications.
- Operational risks related to processes and procedures.
- Compliance with relevant regulations (e.g., HIPAA, SOC 2).
```

- --Remediation:-- Identified risks will be documented, prioritized, and addressed according to their potential impact and likelihood. Remediation plans will be developed and implemented, with progress tracked and reported to senior management via a risk register. Remediation efforts will be documented, including exceptions and compensating controls where applicable.
- --SOC 2 Alignment:-- Risk assessments will specifically identify risks relevant to each of the SOC 2 Trust Services Criteria. For example, risks related to unauthorized access will be mapped to the Security criteria, while risks related to system downtime will be mapped to the Availability criteria.

3. Vulnerability Management

[Organization Name] will maintain a robust vulnerability management program to identify, assess, and remediate security vulnerabilities in our systems and applications.

- --Vulnerability Scanning:-- Regular vulnerability scans will be conducted on all systems and applications using industry-standard scanning tools. Scans will be performed at least quarterly, and more frequently for critical systems. Authenticated and unauthenticated scans will be utilized where appropriate.
- --Patch Management:-- A formal patch management process will be implemented to ensure that security patches are applied promptly and effectively. Patches will be tested in a non-production environment before being deployed to production systems. A risk-based approach will be used to prioritize patching, with critical vulnerabilities addressed within [defined timeframe, e.g., 72 hours] and high vulnerabilities addressed within [defined timeframe, e.g., 30 days]. Exception requests must be formally documented and approved.
- --Vulnerability Assessment:-- Identified vulnerabilities will be assessed to determine their potential impact and likelihood of exploitation. Assessments will consider factors such as CVSS scores, exploit availability, and the sensitivity of the affected data. Penetration testing will be conducted annually by a qualified third party to validate the effectiveness of security controls and identify exploitable vulnerabilities.
- --Remediation Tracking:-- All identified vulnerabilities will be tracked and remediated in a timely manner. Remediation efforts will be documented, and progress will be reported to senior management. A vulnerability register will be maintained to track the status of all identified vulnerabilities.
- --SOC 2 Alignment:-- The vulnerability management program directly supports the Security criteria of SOC 2 by ensuring that vulnerabilities are identified and remediated in a timely manner, reducing the risk of unauthorized access and data breaches. Specific SOC 2 controls supported include CC6.1 (logical access controls) and CC7.1 (configuration management).

4. Data Protection

[Organization Name] is committed to protecting the confidentiality, integrity, and availability of all data, especially PHI.

- --Data Classification:-- Data will be classified based on its sensitivity and criticality. This classification will dictate the appropriate security controls for storage, access, and transmission. Data classification levels will include, but are not limited to: Public,

Internal, Confidential, and Restricted.

- --Data Encryption:-- Sensitive data, both in transit and at rest, will be encrypted using industry-standard encryption algorithms. Encryption keys will be securely managed using a key management system. Acceptable encryption algorithms include:
- --Data at Rest:-- AES-256 (Advanced Encryption Standard) or higher.
- --Data in Transit:-- TLS 1.2 or higher. Strong ciphersuites must be configured.

Encryption keys will be stored separately from the encrypted data. Key management will adhere to NIST Special Publication 800-57.

- --Data Loss Prevention (DLP):-- DLP measures will be implemented to prevent the unauthorized disclosure or loss of sensitive data. This includes monitoring data movement, controlling access to sensitive files, and educating users on data handling best practices. DLP solutions will be configured to monitor for sensitive data patterns and prevent data exfiltration through email, web browsing, and removable media.
- --Data Backup and Recovery:-- Regular backups of critical data will be performed and stored in a secure, offsite location. Data recovery procedures will be documented and tested at least annually to ensure business continuity and disaster recovery. Backup retention policies will be defined based on regulatory requirements and business needs. RTO (Recovery Time Objective) and RPO (Recovery Point Objective) will be defined for critical systems.
- --Data Retention and Disposal:-- Data will be retained only as long as necessary for business or legal requirements, adhering to HIPAA guidelines for PHI. Data will be securely disposed of using methods that prevent unauthorized access or recovery, such as data wiping or physical destruction. A data retention schedule will be maintained.
- --SOC 2 Alignment:-- Data protection measures are critical for meeting the Confidentiality and Privacy criteria of SOC 2. Encryption, access controls, and DLP measures specifically support control CC6.6 (protection of confidentiality of information). Data backup and recovery procedures support the Availability criterion by ensuring business continuity in the event of a disaster (CC4.1 Business Continuity).

5. Access Controls

Access to systems and data will be restricted based on the principle of least privilege.

- --User Account Management:-- User accounts will be created, managed, and terminated according to a defined process. Strong passwords and multi-factor authentication (MFA) will be required for all user accounts accessing sensitive systems and data. Password complexity requirements will include: [Specify requirements, e.g., Minimum 12 characters, upper and lower case letters, numbers, and symbols]. Passwords will be rotated every [defined timeframe, e.g., 90 days].
- --Role-Based Access Control (RBAC):-- Access permissions will be granted based on job roles and responsibilities. Access rights will be reviewed and updated at least annually, and upon any changes to job responsibilities.
- --Privileged Access Management (PAM):-- Access to privileged accounts will be strictly controlled and monitored using a PAM solution. Privileged access will be granted only when necessary and will be subject to enhanced security measures, such as just-in-time access and session recording.
- --Remote Access:-- Remote access to [Organization Name]'s network will be secured using

VPNs and MFA. Remote access policies will be enforced to ensure secure connections and data transmission. Approved VPN protocols include: [Specify approved protocols, e.g., IPSec, OpenVPN].
- --Physical Security:-- Physical access to data centers, server rooms, and other sensitive areas will be restricted and monitored using access control systems, surveillance cameras, and security personnel. Access logs will be reviewed regularly.
- --SOC 2 Alignment:-- Access controls are fundamental to the Security criteria of SOC 2. User account management, RBAC, and PAM directly support control CC6.1 (logical access controls). Physical security measures support control CC6.2 (physical access controls). Regular review of access rights helps ensure ongoing compliance.

6. Incident Response

[Organization Name] will maintain a comprehensive incident response plan to detect, analyze, contain, eradicate, and recover from cybersecurity incidents.

- --Incident Detection:-- Systems and networks will be monitored for suspicious activity using Security Information and Event Management (SIEM) systems and intrusion detection/prevention systems (IDS/IPS). Alerts will be triaged by a security operations center (SOC) or designated security personnel.
- --Incident Reporting:-- All suspected security incidents must be reported immediately to the designated incident response team via [defined reporting method, e.g., helpdesk, email, phone].
- --Incident Response Team:-- A dedicated incident response team will be responsible for investigating and responding to security incidents. The team will include representatives from IT, security, legal, and communications.
- --Incident Response Procedures:-- The incident response plan will outline detailed procedures for handling different types of security incidents, including data breaches, malware infections, ransomware attacks, and system outages. The plan will be tested at least annually through tabletop exercises and simulated incidents.
- --Post-Incident Review:-- Following a security incident, a post-incident review will be conducted to identify the root cause of the incident, evaluate the effectiveness of the incident response plan, and implement corrective actions to prevent future incidents.
- --Notification Procedures:-- The incident response plan will include procedures for notifying affected parties, including patients, regulators (e.g., HHS for HIPAA breaches), and law enforcement, as required by law and regulations. Notification timelines will adhere to regulatory requirements.
- --SOC 2 Alignment:-- The incident response plan supports the Security and Availability criteria of SOC 2. It ensures that security incidents are detected, responded to, and resolved in a timely manner, minimizing the impact on system availability and data confidentiality (CC5.5 Incident Response). Post-incident reviews facilitate continuous improvement of security controls.

7. Change Management

[Organization Name] will implement a formal change management process to ensure that all changes to our IT environment are properly planned, tested, and implemented in a secure manner.

- --Change Request Process:-- All changes to systems, applications, and infrastructure must be submitted through a formal change request process. The change request must include a detailed description of the proposed change, the reason for the change, the potential impact of the change, and a backout plan.
- --Change Approval:-- Change requests must be reviewed and approved by a change management board (CAB), which will include representatives from IT, security, and other relevant departments. The CAB will assess the risks associated with the change and ensure that it is aligned with the organization's security policies and procedures.
- --Testing and Validation:-- All changes must be thoroughly tested in a non-production environment before being deployed to production. Testing should include functional testing, security testing, and performance testing.
- --Implementation and Monitoring:-- Changes will be implemented according to a defined schedule and will be monitored closely to ensure that they are implemented correctly and that they do not have any unintended consequences.
- --Documentation:-- All changes will be documented in a change log, including the date of the change, the person who made the change, and the reason for the change.
- --SOC 2 Alignment:-- Change management supports the Security and Availability criteria of SOC 2. It helps prevent unauthorized or poorly implemented changes that could introduce vulnerabilities or disrupt system availability (CC7.1 Configuration Management).

8. Third-Party Risk Management

[Organization Name] will implement a comprehensive third-party risk management program to assess and mitigate the risks associated with using third-party vendors and business associates.

- --Vendor Due Diligence:-- Before engaging with a third-party vendor, a thorough due diligence process will be conducted to assess their security posture. This includes reviewing their security policies, procedures, and certifications (e.g., SOC 2, ISO 27001), and conducting security questionnaires and risk assessments. A minimum security standard will be established for all vendors handling sensitive data.
- --Contractual Requirements:-- Contracts with third-party vendors will include specific security requirements, such as data protection clauses, incident response obligations, and audit rights. Business Associate Agreements (BAAs) will be in place with all vendors who handle PHI, as required by HIPAA.
- --Ongoing Monitoring:-- The security posture of third-party vendors will be monitored on an ongoing basis through regular reviews of their security performance, vulnerability scans, and penetration tests. Vendors will be required to provide evidence of their compliance with security requirements.
- --Vendor Risk Rating:-- Each vendor will be assigned a risk rating based on the sensitivity of the data they handle, their access to our systems, and their overall security posture. Vendors with higher risk ratings will be subject to more frequent and rigorous monitoring.
- --Termination Procedures:-- Contracts with third-party vendors will include procedures for terminating the relationship in the event of a security breach or other violation of the security requirements. Procedures for secure data return or destruction will be defined.
- --SOC 2 Alignment:-- Third-party risk management is essential for maintaining the

Security, Availability, and Confidentiality criteria of SOC 2. It ensures that third-party vendors meet the organization's security standards and protect sensitive data (CC8.1 Third Party Risk Management).

9. Security Awareness Training

All employees, contractors, and vendors will receive regular security awareness training to educate them about cybersecurity threats and best practices.

- --Training Content:-- Training will cover topics such as:
- Phishing awareness.
- Password security.
- Data handling procedures.
- Social engineering.
- Incident reporting.
- Acceptable use of company resources.
- HIPAA compliance (for those handling PHI).
- Secure coding practices (for developers).
- --Training Frequency:-- Security awareness training will be conducted at least annually, and more frequently for high-risk individuals (e.g., those with privileged access) and new hires.
- --Training Delivery:-- Training will be delivered through a variety of methods, including online modules, in-person presentations, simulated phishing exercises, and security newsletters.
- --Training Tracking:-- Completion of security awareness training will be tracked and reported to management. Training records will be maintained for audit purposes.
- --SOC 2 Alignment:-- Security awareness training supports all of the SOC 2 Trust Services Criteria by educating users about security risks and best practices, reducing the likelihood of human error and security breaches. This specifically supports CC9.1 (security awareness training).

10. Security Governance

[Organization Name] will establish and maintain a security governance framework to provide oversight and direction for our cybersecurity program.

- --Security Committee:-- A security committee will be established, comprising senior management representatives from IT, security, legal, compliance, and other relevant departments. The committee will be responsible for:
- Approving the cybersecurity policy and other security-related documents.
- Reviewing risk assessments and remediation plans.
- Monitoring the effectiveness of security controls.
- Overseeing incident response activities.
- Ensuring compliance with applicable laws, regulations, and industry standards.
- --Security Roles and Responsibilities:-- Clearly defined security roles and responsibilities will be established for all employees, contractors, and vendors.
- --Policy Enforcement:-- This cybersecurity policy will be enforced through a combination of technical controls, administrative procedures, and disciplinary actions.

- --SOC 2 Alignment:-- Security governance is essential for establishing and maintaining a strong security posture and ensuring ongoing compliance with SOC 2 requirements. This section directly relates to and supports control CC1 (Control Environment).

11. Business Continuity and Disaster Recovery

[Organization Name] will maintain a comprehensive business continuity and disaster recovery (BCDR) plan to ensure that critical business functions can continue to operate in the event of a disruption.

- --BCDR Plan:-- The BCDR plan will outline detailed procedures for:
- Identifying critical business functions.
- Assessing the potential impact of disruptions.
- Developing recovery strategies.
- Testing the BCDR plan.
- Maintaining the BCDR plan.
- --Backup and Recovery Procedures:-- Regular backups of critical data will be performed and stored in a secure, offsite location. Data recovery procedures will be documented and tested at least annually to ensure business continuity and disaster recovery.
- --Disaster Recovery Site:-- A disaster recovery site will be maintained to provide a redundant environment for critical systems and applications in the event of a disaster.
- --SOC 2 Alignment:-- Business continuity and disaster recovery planning are essential for meeting the Availability criteria of SOC 2. It ensures that critical business functions can continue to operate in the event of a disruption (CC4.1 Business Continuity).

12. Compliance and Auditing

[Organization Name] is committed to complying with all applicable laws, regulations, and industry standards, including SOC 2, HIPAA, and other relevant regulations.

- --SOC 2 Compliance:-- This policy is designed to support [Organization Name]'s SOC 2 compliance efforts. We will implement and maintain controls to meet the SOC 2 Trust Services Criteria (e.g., Security, Availability, Processing Integrity, Confidentiality, Privacy).
- --HIPAA Compliance:-- We will comply with all applicable HIPAA regulations, including the Privacy Rule, the Security Rule, and the Breach Notification Rule.
- --Internal Audits:-- Regular internal audits will be conducted at least annually to assess the effectiveness of security controls and compliance with this policy. Audit findings will be documented and tracked to resolution.
- --External Audits:-- External audits will be performed by qualified third-party auditors to verify compliance with SOC 2, HIPAA, and other applicable regulations. Audit reports will be reviewed by senior management.
- --Policy Review:-- This policy will be reviewed and updated at least annually, or more frequently as needed to address changes in the threat landscape, regulations, or business operations. The policy review date will be documented.
- --Documentation:-- All security policies, procedures, and controls will be documented and maintained in a central repository. Documentation will be reviewed and updated regularly.

13. Conclusion

This Cybersecurity Policy is essential for protecting [Organization Name]'s information assets and ensuring the privacy and security of patient data. By adhering to this policy, we can mitigate cybersecurity risks, maintain compliance with applicable regulations, and build trust with our patients, partners, and stakeholders. Every member of our organization is responsible for understanding and following this policy.

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. Furthermore, non-compliance may result in legal penalties, financial losses, and reputational damage to the organization. Specific examples of non-compliance consequences include:

- --Unauthorized Disclosure of PHI:-- Termination of employment, civil and criminal penalties under HIPAA.
- --Failure to Report Security Incident:-- Disciplinary action, legal penalties under HIPAA and other applicable laws.
- --Violation of Access Control Policies:-- Suspension of access privileges, disciplinary action, potential legal penalties.

This policy is approved by [Name and Title] and is effective as of [Date].

"""

return revised_prompt
```

Key changes and explanations:

- --Explicit SOC 2 Alignment in Each Section:-- Each section now includes a "--SOC 2 Alignment--" subsection. This is the most important change. It -explicitly- calls out how the controls described in that section map back to specific SOC 2 Trust Services Criteria. I've provided examples (e.g., CC6.1, CC7.1), but these would need to be tailored to the specific controls being implemented in the healthcare organization. This makes the policy much more useful for a SOC 2 audit. I have added references to the specific Common Criteria (CC) within SOC2.
- --Security Governance Section:-- Added a new section on "Security Governance" to address the feedback. This section covers the security committee, roles and responsibilities, and policy enforcement. This is crucial for demonstrating a commitment to security at the highest levels of the organization.
- --Business Continuity and Disaster Recovery Section:-- Added a new section on "Business Continuity and Disaster Recovery" to address the feedback.
- --More Specific Conclusion:-- The "Conclusion" section is expanded to include more specific consequences for non-compliance, giving concrete examples related to PHI disclosure, incident reporting, and access control violations. This makes the policy much stronger and more enforceable. This provides examples of what the consequences of non-compliance can be.
- --Key Management Details:-- Added information about key management adherence to NIST SP 800-57.
- --Language and Tone:-- Maintained a professional and formal tone suitable for an enterprise environment.
```

- --Emphasis on Controls:-- The revisions consistently use the term "controls" and emphasize the implementation and maintenance of controls to meet SOC 2 criteria.
- --Clearer Language:-- Revised some sentences for clarity and readability.

This revised prompt provides a much stronger foundation for generating a cybersecurity policy that is both comprehensive and specifically aligned with SOC 2 requirements. Remember that the example SOC 2 control mappings (CC references) -must- be validated and customized to the specific environment and controls in place. The organization will also want to be explicit in the policy as to what version of SOC2 (e.g., SOC2 + HIPAA) this aligns to.