Okay, I understand. I will focus on replacing placeholders with specific, verifiable requirements, and incorporate all other feedback.

Here's the revised prompt, aiming for a cybersecurity policy that is more concrete and actionable, and addresses the remaining feedback:

Revised Prompt:

You are to generate a comprehensive cybersecurity policy for an organization that is subject to the Data Deletion and Retention Obligation (DDRO) standard (Assume a simplified version for demonstration purposes). The policy must address the following areas, incorporating the specifics outlined below, and address all feedback from the previous review:

1. Purpose:

- State the purpose of the cybersecurity policy, which is to protect the confidentiality, integrity, and availability of the organization's information assets and to ensure compliance with the DDRO.
- Emphasize the importance of data security, access control, incident response, and risk management.

2. Scope:

- Define the scope of the policy, which includes all employees, contractors, vendors, and other third parties who have access to the organization's information assets.
- Specify that the policy applies to all information assets, including data, systems, networks, and physical facilities.

3. Risk Assessment:

- --Asset Identification:-- Identify and classify all critical assets, including servers, databases, workstations, network devices, and data repositories. -Example: All servers hosting Personally Identifiable Information (PII) will be classified as High Criticality and documented in the Asset Inventory maintained by the IT Department.-
- --Threat Identification:-- Identify potential threats to the organization's information assets, including malware, phishing, ransomware, insider threats, and physical security breaches. -Example: Regularly review threat intelligence feeds from [Specific Provider Name] to identify emerging threats targeting the healthcare industry.-
- --Vulnerability Assessment:-- Conduct regular vulnerability assessments to identify weaknesses in the organization's systems and applications using [Specific Vulnerability Scanner Name].
- Vulnerability scans will be performed at least quarterly on all critical systems.
- High-severity vulnerabilities will be remediated within 30 days.
- Medium-severity vulnerabilities will be remediated within 90 days.
- Low-severity vulnerabilities will be addressed during scheduled maintenance windows.
- --Risk Treatment:-- Detail risk treatment strategies, specifying risk acceptance for "Low Risk" categorizations. Given the organization's risk profile as a low-risk entity, risks categorized as 'Low' will be accepted with continuous monitoring.
- --Regular Updates:-- Risk assessments will be reviewed and updated at least annually or

more frequently if there are significant changes to the organization's environment or threat landscape.

4. Data Protection:

- --Data Minimization:-- Limit the collection and retention of personal data to what is necessary for specific, legitimate purposes. Implement processes to regularly review and delete unnecessary data.
- --Encryption:-- Encrypt sensitive data at rest and in transit using strong encryption algorithms (e.g., AES-256).
- All laptops and mobile devices will be encrypted using [Specific Encryption Software Name].
- Data in transit over public networks will be protected using TLS 1.3 or higher.
- Compliance with [DDRO Section 3.2.a - Encryption of PHI: All PHI stored electronically must be encrypted using AES-256 or a stronger algorithm approved by the Data Security Board].
- --Data Loss Prevention (DLP):-- Implement DLP solutions to prevent sensitive data from leaving the organization's control. DLP will monitor outbound email for attachments containing social security numbers, patient names, and medical record numbers. DLP events will be reviewed daily by the Security Team.
- --Data Backup and Recovery:-- Implement regular data backups and recovery procedures to ensure business continuity in the event of a disaster. Backups will be stored offsite and tested quarterly. The Recovery Time Objective (RTO) for critical systems is 4 hours, and the Recovery Point Objective (RPO) is 1 hour.
- --Data Retention and Disposal:-- Establish data retention and disposal policies to ensure that data is not retained longer than necessary and is securely disposed of when it is no longer needed. Compliance with [DDRO Section 4.1.b - Data Retention: Personal data shall not be retained for longer than 7 years after the last date of service]. Secure data destruction methods will be used, such as data wiping or physical destruction of storage media.
- --Physical Record Security:-- Physical records containing sensitive information will be stored in locked cabinets and access will be limited to authorized personnel. Physical records will be shredded when they are no longer needed.

5. Access Control:

- --Strong Authentication:-- Implement strong authentication mechanisms, such as multi-factor authentication (MFA), for all users. All users will be required to use MFA for access to corporate email, VPN, and critical applications using [Specific MFA Solution Name].
- --Role-Based Access Control (RBAC):-- Implement RBAC to ensure that users only have access to the information and resources they need to perform their job duties. User access will be reviewed quarterly by department managers.
- --Access Reviews:-- Conduct regular access reviews to ensure that user access is still appropriate and necessary. The IT Department will conduct access reviews quarterly.
- --Privileged Access Management (PAM):-- Implement PAM solutions to control and monitor access to privileged accounts using [Specific PAM Solution Name].

- --Account Management:-- Implement procedures for creating, modifying, and disabling user accounts. Employee accounts will be disabled within 24 hours of termination.
- --Physical Access Control:-- Implement physical access controls to protect the organization's facilities and information assets. Access to the data center will be restricted to authorized personnel only, and access will be logged. [Specific Access Control System Name] is in place.

6. Incident Response:

- A comprehensive incident response plan will be maintained to address security incidents in a timely and effective manner. The plan will be tested annually through tabletop exercises. This aligns with [DDRO Incident Reporting requirements, e.g., DDRO Section 5.1.a - All breaches of PHI affecting more than 500 individuals must be reported to the DDRO within 60 days of discovery]. The plan will include:

- --Incident Severity Levels:-- Incidents will be classified into the following severity levels:
- Critical: Confirmed breach of PHI affecting more than 500 individuals, system-wide ransomware infection, or significant disruption of critical business operations. Response: Immediate notification of Privacy Officer and regulatory agencies (if applicable), activation of the Incident Response Team, and implementation of containment measures.
- High: Confirmed breach of PHI affecting fewer than 500 individuals, targeted malware infection, or significant vulnerability identified in a critical system. Response: Activation of the Incident Response Team, implementation of containment measures, and remediation of the vulnerability.
- Medium: Suspected breach of PHI, minor malware infection, or vulnerability identified in a non-critical system. Response: Investigation by the IT Security Team, implementation of containment measures (if necessary), and remediation of the vulnerability.
- Low: Suspicious activity with no confirmed breach, minor technical issues, or policy violations. Response: Investigation by the IT Security Team and corrective action (if necessary).

- --Incident Detection:-- Monitoring systems and networks for suspicious activity and potential security incidents using Security Information and Event Management (SIEM) system [Specific SIEM Name]. Alerts will be configured to detect common attack patterns.

- --Incident Reporting:-- Establishing a clear process for reporting security incidents. All employees are responsible for reporting any suspected security incidents immediately to the IT Helpdesk at [Phone Number] or [Email Address]. The Helpdesk will then escalate the incident to the Incident Response Team.

- --Incident Response Team:-- Designating an incident response team with clearly defined roles and responsibilities.
- IT Security Lead: [Name and Contact Information]
- Privacy Officer: [Name and Contact Information]
- Legal Counsel: [Name and Contact Information]
- --Communication Protocols:-- During a Critical or High severity incident, the Communications Lead will be responsible for notifying the following parties within the

specified timeframes:

- Internal:
- Privacy Officer: Immediately
- Executive Management: Within 1 hour
- Legal Counsel: Within 1 hour
- Affected Department Heads: Within 4 hours
- External:
- Regulatory Agencies (if applicable): Within [DDRO Required Timeframe - e.g., 60 days]
- Affected Individuals (if applicable): Within [Legal/Regulatory Timeframe - e.g., 60 days]

- --Incident Containment:-- Implementing measures to contain the impact of a security incident. This may include isolating affected systems, disabling compromised accounts, and blocking malicious traffic.

- --Incident Eradication:-- Removing the cause of a security incident.

- --Incident Recovery:-- Restoring systems and data to normal operations.

- --Legal Hold:-- Upon notification of a potential legal issue related to an incident, Legal Counsel will issue a legal hold notice. The IT Department will then implement procedures to preserve all potentially relevant data, including email, system logs, and database records.

- --Post-Incident Analysis:-- Conducting a post-incident analysis to identify the root cause of the incident and improve security controls.

The incident response plan is located at [Location of Incident Response Plan] and will be reviewed and updated [Frequency - e.g., Annually].

7. Security Awareness Training:

- Provide regular security awareness training to all employees and contractors. The training will cover topics such as password security, phishing awareness, malware awareness, data protection, and incident reporting. Training will be conducted annually, and new employees will receive training within 30 days of hire.
- Specific Training Modules:
- Password Security: Creating strong passwords and avoiding password reuse.
- Phishing Awareness: Identifying and avoiding phishing attacks.
- Malware Awareness: Recognizing and preventing malware infections.
- Data Protection: Protecting sensitive data and complying with data protection policies.

8. Physical Security and Environmental Controls:

- Implement physical security measures to protect the organization's facilities and information assets.
- All facilities will have controlled access points with [Specific Access Control System Name].
- Security cameras will be installed in critical areas.
- Visitor Management: All visitors must sign in at the reception desk, present a valid photo ID, and be escorted by an employee at all times. A visitor log will be maintained for 1

year.
- Implement environmental controls to protect the organization's systems and data from environmental hazards, such as temperature and humidity.
- The data center will be equipped with temperature and humidity sensors with automated alerts that trigger when conditions deviate from acceptable ranges.
- Fire suppression systems will be installed in all facilities.

9. Compliance and Auditing:

- Establish procedures for ensuring compliance with the DDRO and other relevant regulations.
- Conduct regular internal and external audits to assess the effectiveness of the cybersecurity policy and identify areas for improvement.
- --Audit Scope:-- Internal audits will cover all areas of the cybersecurity policy, including risk assessment, data protection, access control, incident response, and physical security. External audits will be conducted by a qualified third-party auditor.
- --Remediation of Audit Findings:-- A process will be in place to track and remediate audit findings. The IT Security Manager will be responsible for tracking and remediating audit findings.
- Compliance with [DDRO Section 6.2.c - Audit Trail Retention: Audit trails shall be retained for a period of no less than 3 years].

10. Policy Enforcement:

- Clearly state the consequences of violating the cybersecurity policy, including disciplinary action up to and including termination of employment.

11. Version Control:

- --Version Number:-- 1.0
- --Date of Last Revision:-- 2023-10-27
- --Description of Changes:-- Initial draft of cybersecurity policy.

12. Definitions:

- --PHI:-- Protected Health Information.
- --Malware:-- Malicious software.
- --Vulnerability:-- A weakness in a system or application that could be exploited by a threat.

Output:

Generate a document representing a full cybersecurity policy based on the above specifications. This should be a standalone, ready-to-implement policy document. Pay very close attention to replacing bracketed placeholders with real or reasonably representative information.