Okay, here's the revised Cybersecurity Policy, incorporating the feedback provided. I've focused on adding detail, specifics, and a mapping of policy elements to DDRO requirements where appropriate.

```

## Cybersecurity Policy for Operations - Low Risk Environment

### 1. Introduction

This Cybersecurity Policy outlines the standards and procedures implemented to protect the confidentiality, integrity, and availability of information assets within our Operations environment. This policy is designed to address the specific risks associated with our industry while acknowledging the assessment of a "Low Risk" operating environment. All employees, contractors, vendors, and any other individuals with access to our systems and data are expected to adhere to this policy. This policy supports our commitment to responsible data handling and compliance with applicable regulations, including the DDRO compliance standard.  This policy will be reviewed and updated at least annually, or more frequently in response to significant changes in the threat landscape, business operations, or regulatory requirements.

### 2. Risk Assessment

Due to the identified "Low Risk" environment, we will conduct risk assessments on an annual basis, or more frequently if significant changes occur in our operational environment, threat landscape, or regulatory requirements. These assessments will identify potential threats, vulnerabilities, and their potential impact on our business operations. While the overall risk is deemed low, the assessments will still consider factors such as:

- --Data Sensitivity:-- Identifying the classification of data handled (e.g., Public, Internal, Confidential, Restricted).  Specific classifications will be defined in a Data Classification Standard.
- --System Criticality:-- Determining the importance of IT systems to business operations (e.g., mission-critical, business-critical, support systems). This assessment will consider the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each system.
- --Threat Landscape:-- Monitoring for emerging threats relevant to our industry and business profile, using sources such as industry-specific threat intelligence feeds and vulnerability databases (e.g., NIST National Vulnerability Database).
- --Vulnerability Scanning:-- Regularly scanning systems for known vulnerabilities using automated vulnerability scanners (e.g., Nessus Essentials) and penetration testing, at least annually.

The risk assessment findings will be documented in a Risk Register, which will include identified risks, their likelihood and impact, proposed mitigation strategies, and assigned owners. This register will be reviewed and updated regularly.

### 3. Data Protection

Despite operating in a low risk environment, data protection is paramount. The following measures are in place:
```

- --Data Classification:-- Data will be classified based on sensitivity and business value according to the Data Classification Standard. Examples include:
- -Public:- Information freely available to anyone.
- -Internal:- Information for internal use only.
- -Confidential:- Information requiring protection due to legal or competitive reasons.
- -Restricted:- Highly sensitive information requiring the highest level of protection.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to data handling and classification, specifically [Insert specific DDRO clause number related to data classification].

- --Data Storage:-- Data will be stored securely using appropriate physical and logical controls, including encryption where deemed necessary based on data classification. For example:
- -Confidential and Restricted data- at rest will be encrypted using AES-256 encryption. Storage locations will be physically secured with access restricted to authorized personnel.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to data handling and storage, specifically [Insert specific DDRO clause number related to data storage and encryption].

- --Data Transmission:-- Sensitive data transmitted electronically will be protected using encryption protocols such as TLS 1.3 or higher for web traffic and secure email protocols (e.g., S/MIME) for email communication.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to data transmission, specifically [Insert specific DDRO clause number related to data transmission].

- --Data Backup and Recovery:-- Regular backups of critical data will be performed and stored securely offsite in an encrypted format. A documented recovery plan will be maintained and tested at least annually to ensure data recoverability within defined RTOs and RPOs. The backup retention policy will be defined based on legal and business requirements.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to data backup and recovery, specifically [Insert specific DDRO clause number related to data backup and recovery].

- --Data Disposal:-- Data will be securely disposed of using methods that prevent unauthorized access. This includes:
- -Electronic data:- Data wiping using secure wiping tools (e.g., DBAN) that overwrite data multiple times.
- -Physical media:- Physical destruction of storage media (e.g., shredding hard drives).
- -Paper documents:- Shredding confidential documents.

A documented data disposal procedure will be maintained.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to data

disposal, specifically [Insert specific DDRO clause number related to data disposal].

4. Access Controls

Access to systems and data will be granted based on the principle of least privilege. The following access control measures are implemented:

- --User Authentication:-- Strong passwords (minimum 12 characters, including upper and lower case letters, numbers, and symbols) will be required for all users. Multi-factor authentication (MFA) will be implemented for all privileged accounts and for remote access.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to access control and authentication, specifically [Insert specific DDRO clause number related to access control and authentication].

- --Role-Based Access Control (RBAC):-- Access permissions will be assigned based on job roles and responsibilities. A matrix defining roles and associated access rights will be maintained.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to access control and authorization, specifically [Insert specific DDRO clause number related to Role-Based Access Control].

- --Account Management:-- User accounts will be created, modified, and terminated promptly according to a documented account management procedure. Regular reviews of user access rights will be conducted quarterly. Dormant accounts will be disabled and eventually deleted.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to account management, specifically [Insert specific DDRO clause number related to account management].

- --Remote Access:-- Secure methods, such as VPNs with MFA, will be used for remote access to the network. Remote access will be limited to authorized personnel and require justification.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to Remote Access, specifically [Insert specific DDRO clause number related to Remote Access].

- --Physical Security:-- Physical access to IT infrastructure (servers, networking equipment) will be restricted to authorized personnel only. Access will be controlled using access cards or biometric authentication. Visitor access will be logged and monitored.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to Physical Security, specifically [Insert specific DDRO clause number related to Physical Security].

5. Incident Response

Even in a low risk environment, it is crucial to have procedures in place to effectively manage security incidents. An Incident Response Plan (IRP) will be maintained, regularly

reviewed (at least annually), and tested (tabletop exercises annually) to ensure its effectiveness. The IRP will be a separate document that outlines the steps to be taken in the event of a security incident, including:

- --Incident Identification:-- Procedures for identifying and reporting potential security incidents. This includes establishing a dedicated email address (security@example.com) and a hotline for reporting incidents. All employees are responsible for reporting suspected security incidents immediately.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to incident reporting, specifically [Insert specific DDRO clause number related to incident reporting].

- --Incident Containment:-- Measures to contain the impact of a security incident, such as isolating affected systems from the network.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to incident containment, specifically [Insert specific DDRO clause number related to incident containment].

- --Incident Eradication:-- Steps to remove the cause of the incident, such as patching vulnerabilities or removing malware.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to incident eradication, specifically [Insert specific DDRO clause number related to incident eradication].

- --Incident Recovery:-- Procedures for restoring systems and data to normal operation, including restoring from backups if necessary.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to incident recovery, specifically [Insert specific DDRO clause number related to incident recovery].

- --Post-Incident Analysis:-- A review of the incident to identify lessons learned and improve security controls. A post-incident report will be created and shared with relevant stakeholders.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to post-incident analysis, specifically [Insert specific DDRO clause number related to post-incident analysis].

The IRP will define roles and responsibilities for incident response team members, including a designated Incident Commander.

6. Security Awareness Training

All employees will receive security awareness training upon hire and annually thereafter. Training will cover topics such as:

- --Password Security:-- Creating and maintaining strong passwords, using password managers, and avoiding password reuse.
- --Phishing Awareness:-- Recognizing and avoiding phishing scams, identifying suspicious

emails, and reporting phishing attempts. Simulated phishing campaigns will be conducted periodically to assess employee awareness.
- --Data Handling:-- Proper procedures for handling and protecting sensitive data, including data classification and secure data disposal.
- --Incident Reporting:-- Procedures for reporting security incidents and the importance of timely reporting.
- --Social Engineering:-- Recognizing and avoiding social engineering attacks, such as pretexting and baiting.
- --Mobile Device Security:-- Securing mobile devices used for work purposes, including password protection, encryption, and remote wiping capabilities.

The training will be tailored to the specific risks and threats relevant to our Operations environment, despite it's low risk profile. Training records will be maintained.

--DDRO Alignment:-- This section directly addresses DDRO requirements related to security awareness and training, specifically [Insert specific DDRO clause number related to training].

7. Compliance and Auditing

We are committed to complying with all applicable laws, regulations, and industry standards, including DDRO.

- --DDRO Compliance:-- We will implement and maintain controls necessary to achieve and maintain compliance with the DDRO standard. Specifically:

- -Data Handling:- As detailed in Section 3, we implement data classification, encryption, and secure disposal procedures to meet DDRO's data handling requirements. [Insert specific DDRO clause number(s)].
- -Access Controls:- As detailed in Section 4, we implement strong authentication, RBAC, and account management practices to meet DDRO's access control requirements. [Insert specific DDRO clause number(s)].
- -Incident Reporting:- As detailed in Section 5, we maintain an Incident Response Plan and procedures for identifying, reporting, and responding to security incidents to meet DDRO's incident reporting requirements. [Insert specific DDRO clause number(s)].
- -Training:- As detailed in Section 6, we provide security awareness training to our employees to ensure they understand their responsibilities for protecting information. [Insert specific DDRO clause number(s)].

- --Internal Audits:-- Regular internal audits will be conducted at least annually to assess the effectiveness of our security controls and compliance with this policy and relevant regulations. Audit findings will be documented and tracked to remediation.

- --External Audits:-- Periodic external audits may be conducted to provide independent assurance of our security posture and compliance with applicable standards.

8. Conclusion

This Cybersecurity Policy is a critical component of our overall risk management strategy. While our environment is categorized as "Low Risk," adherence to this policy is essential

to protect our information assets and maintain the trust of our stakeholders. This policy will be reviewed and updated periodically to ensure it remains relevant and effective in addressing evolving threats and regulatory requirements. The CISO (or designated Security Officer) is responsible for the implementation and enforcement of this policy, with support from all employees and stakeholders. Exceptions to this policy must be documented and approved by the CISO.
```

Key improvements and explanations:

- --More Specific Examples:-- Added examples of encryption standards (AES-256, TLS 1.3), data wiping tools (DBAN), vulnerability scanners (Nessus), and remote access methods (VPN with MFA).
- --Concrete Procedures:-- Expanded on data disposal methods, backup procedures (including retention policy), and account management practices.
- --Incident Response Detail:-- While maintaining the reference to a separate IRP, the policy now includes a high-level overview of the key components -within- the policy itself.
- --DDRO Mapping:--  The most significant change is the explicit mapping of policy sections to specific DDRO requirements.  Crucially, the instructions now include placeholders: `[Insert specific DDRO clause number(s)]`.  --You MUST replace these placeholders with the -actual- DDRO clause numbers that each section addresses.-- This is -essential- for demonstrating actual compliance.  I have aligned specific sections of the policy that are addressing requirements to the corresponding areas of DDRO (data handling, access controls, incident reporting and training)
- --Policy Review:--  Added frequency and reasons for policy review.
- --Exception Handling:--  Added requirement for documented and approved exceptions.
- --Added Specificity:-- Added more specific data types that are classified.
- --Clarity and Readability:-- Enhanced the language for better clarity and understanding.

--Important Considerations:--

- --DDRO Clause Numbers:--  --The placeholders for DDRO clause numbers -must- be replaced with the actual numbers from the DDRO standard.-- This is the most critical step in making this policy truly compliant.  You will need to consult the DDRO documentation to find the relevant clauses.
- --Tailoring:--  This is still a general template. You need to tailor it to your specific organization, systems, data, and risk profile.
- --Supporting Documentation:-- This policy will likely require supporting documentation, such as:
- Data Classification Standard
- Incident Response Plan
- Account Management Procedure
- Data Disposal Procedure
- Risk Register
- --Legal Review:-- It is strongly recommended to have this policy reviewed by legal counsel to ensure it complies with all applicable laws and regulations.
```

- --Enforcement:-- Having a policy is not enough. You must enforce it consistently and fairly.
- --Low Risk Justification:-- Ensure the "Low Risk" assessment is properly documented and justifiable. The regulators may challenge this assessment if the controls are weak or if there is evidence of significant risk. Document -why- it's considered low risk.
- --CISO or Designated Security Officer:-- Clearly identify the role responsible for the enforcement of this policy.

By addressing the weaknesses identified and adding the necessary specifics and DDRO mapping, this revised Cybersecurity Policy should be a significantly more robust and effective document. Remember to fill in the DDRO clause numbers and tailor the policy to your organization's unique context.