Okay, here's a comprehensive cybersecurity policy revised based on your feedback, aiming for a "low-risk" environment in the IT industry and alignment with ISO/IEC 27001. I've addressed the specifics you highlighted in your evaluation.

--Cybersecurity Policy--

--1. Introduction--

This Cybersecurity Policy outlines the principles, standards, and procedures that [Company Name] follows to protect the confidentiality, integrity, and availability of its information assets. This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing or using [Company Name]'s information systems, networks, and data, regardless of location.

The purpose of this policy is to:

- Establish a framework for managing cybersecurity risks.
- Protect sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Ensure compliance with applicable laws, regulations, and industry standards, including alignment with ISO/IEC 27001.
- Maintain the trust of our customers, partners, and stakeholders.

While [Company Name] operates in a low-risk environment, proactive cybersecurity measures are essential to prevent and mitigate potential threats. This policy is reviewed and updated at least annually, or more frequently as needed, to adapt to evolving threats and business changes.

--2. Risk Assessment--

[Company Name] recognizes the importance of identifying and managing cybersecurity risks. Our risk assessment process is designed to be consistent with ISO/IEC 27005 guidelines.

- --Methodology:-- We utilize a semi-quantitative risk assessment methodology. This involves:
- --Asset Identification:-- Identifying critical information assets, including data, systems, and networks.
- --Threat Identification:-- Identifying potential threats that could exploit vulnerabilities in our assets. This includes malware, phishing, social engineering, and unauthorized access.
- --Vulnerability Assessment:-- Evaluating weaknesses in our systems and processes that could be exploited by threats.
- --Impact Analysis:-- Assessing the potential impact of a successful attack, considering factors such as financial loss, reputational damage, legal liabilities, and operational disruption.
- --Likelihood Assessment:-- Determining the probability of a threat exploiting a vulnerability.
- --Risk Scoring:-- Combining impact and likelihood to assign a risk score to each identified risk.
- --Risk Register:-- A Risk Register is maintained to document identified risks, their

potential impact, likelihood, assigned risk scores, and mitigation strategies.

- --Roles and Responsibilities:--
- --IT Department:-- Responsible for conducting regular risk assessments, implementing security controls, and monitoring for security incidents.
- --Management Team:-- Responsible for reviewing and approving risk assessment results, allocating resources for risk mitigation, and ensuring compliance with this policy.
- --All Employees:-- Responsible for reporting any suspected security vulnerabilities or incidents.
- --Risk Appetite and Tolerance:-- [Company Name] has a -conservative- risk appetite. We aim to minimize exposure to cybersecurity risks and are willing to invest resources to mitigate potential threats, even those with low likelihood. Our risk tolerance is defined as the acceptable level of residual risk -after- implementing mitigation measures. Specific risk tolerance levels are documented within the Risk Register for each asset. This tolerance will be reassessed and changed upon new threat information.
- --Regular Assessments:-- Risk assessments are conducted at least annually, or more frequently if there are significant changes to our business operations, technology infrastructure, or threat landscape. Penetration tests and vulnerability scans are conducted quarterly, or sooner if there is a new, critical vulnerability is discovered.
- --Low-Risk Environment Considerations:-- While we classify our environment as "low-risk," this refers to the -inherent risk- based on the nature of our business and the sensitivity of our data. However, we acknowledge that even low-risk environments are susceptible to attacks, and this policy implements appropriate security controls to mitigate those risks.

--3. Data Protection--

[Company Name] is committed to protecting the confidentiality, integrity, and availability of all data entrusted to us.

- --Data Classification:-- Data is classified based on its sensitivity and criticality to the organization. Classifications include:
- --Public:-- Information freely available to the public.
- --Internal:-- Information intended for internal use only.
- --Confidential:-- Sensitive information that requires strict protection, such as customer data, financial records, and trade secrets.
- --Data Handling Procedures:-- Specific procedures are in place for handling each data classification. These procedures address:
- --Storage:-- Where data can be stored (e.g., encrypted hard drives, secure cloud storage).
- --Transmission:-- How data can be transmitted (e.g., encrypted email, secure file transfer protocols).
- --Access:-- Who has access to data (see Section 4, Access Controls).
- --Disposal:-- How data is securely disposed of when it is no longer needed (e.g., secure data wiping, physical destruction of media).
- --Encryption:-- Encryption is used to protect sensitive data at rest and in transit. Specific encryption standards (e.g., AES-256) are used for data stored on servers and workstations. All network traffic is encrypted using TLS/SSL.
- --Data Backup and Recovery:-- Regular backups are performed to ensure data can be

recovered in the event of a disaster or data loss. Backup data is stored in a secure, offsite location. Backup and recovery procedures are tested regularly.

- --Data Loss Prevention (DLP):-- DLP tools and processes are used to prevent sensitive data from leaving the organization without authorization.
- --Privacy:-- [Company Name] complies with all applicable privacy laws and regulations. A Privacy Policy is maintained to inform individuals about how their personal information is collected, used, and protected.

--4. Access Controls--

[Company Name] implements robust access controls to restrict access to information systems and data to authorized users only.

- --Least Privilege:-- Users are granted only the minimum level of access required to perform their job duties.
- --Strong Authentication:-- Multi-factor authentication (MFA) is required for all users accessing internal systems and data remotely, and for privileged accounts accessing sensitive systems. MFA leverages technologies such as:
- Authenticator Apps (e.g. Google Authenticator, Microsoft Authenticator)
- Hardware Tokens (e.g. YubiKey)
- SMS-based Verification (used as a last resort)
- --Role-Based Access Control (RBAC):-- Access rights are assigned based on job roles, rather than individual users. This simplifies access management and ensures consistency.
- --Privileged Access Management (PAM):-- PAM solutions are used to control and monitor access to privileged accounts. This includes:
- Secure storage and rotation of privileged credentials.
- Auditing of privileged user activity.
- Just-in-time (JIT) access provisioning.
- --Password Management:--
- --Complexity:-- Passwords must meet the following complexity requirements:
- Minimum length of 12 characters.
- Include a combination of uppercase and lowercase letters, numbers, and symbols.
- Not be based on personal information (e.g., names, birthdays).
- Not be reused from previous passwords.
- --Expiration:-- Passwords must be changed every 90 days.
- --Storage:-- Passwords must be stored securely using a strong hashing algorithm.
- --Access Logging and Monitoring:-- All access to information systems and data is logged and monitored for suspicious activity. Logs are reviewed regularly to identify potential security incidents. Access logs are retained for at least 12 months.
- --Account Management:--
- User accounts are created and managed through a centralized identity management system.
- New accounts are created only after proper authorization.
- Accounts are disabled promptly when employees leave the organization or change roles.
- Inactive accounts are automatically disabled after 90 days of inactivity.
- --Network Segmentation:-- Networks are segmented to isolate critical systems and data from less secure areas. Firewalls and other security controls are used to restrict traffic between network segments.

--5. Incident Response--

[Company Name] has a documented Incident Response Plan (IRP) to effectively respond to and recover from cybersecurity incidents. The IRP is tested annually.

- --Incident Reporting:-- All employees are responsible for reporting any suspected security incidents immediately to the IT Department.
- --Incident Triage:-- The IT Department will triage reported incidents to determine their severity and impact.
- --Containment:-- If an incident is confirmed, the IT Department will take immediate steps to contain the incident and prevent further damage.
- --Eradication:-- The IT Department will work to eradicate the root cause of the incident.
- --Recovery:-- The IT Department will restore affected systems and data to their normal operating state.
- --Post-Incident Activity:-- A post-incident review will be conducted to identify lessons learned and improve our security posture.
- --Roles and Responsibilities:-- The Incident Response Team comprises the following roles:
- --Incident Commander:-- The Incident Commander (usually the IT Manager) is responsible for leading the incident response effort, coordinating team activities, and making critical decisions.
- --Communications Officer:-- The Communications Officer is responsible for communicating with internal and external stakeholders, including employees, customers, and law enforcement (if necessary).
- --Technical Lead:-- The Technical Lead (usually a Senior IT Engineer) is responsible for providing technical expertise, conducting forensic analysis, and implementing technical solutions to contain and eradicate incidents.
- --Legal Counsel:-- The Legal Counsel provides guidance on legal and regulatory compliance issues related to the incident.
- --Escalation Procedures:--
- Incidents are escalated based on their severity and impact.
- Minor incidents are handled by the IT Department.
- Major incidents (e.g., data breaches, system outages) are escalated to the Management Team.
- In the event of a suspected criminal activity, law enforcement will be notified.
- --Incident Documentation:-- All incident response activities are documented in detail, including the date and time of the incident, the nature of the incident, the steps taken to contain and eradicate the incident, and the impact of the incident.
- --Communication Plan:-- A communication plan is in place to ensure timely and effective communication during a security incident.

--6. Security Awareness Training--

[Company Name] provides regular security awareness training to all employees to educate them about cybersecurity threats and best practices.

- --Training Content:-- Training covers topics such as:
- Phishing awareness.
- Password security.

- Social engineering.
- Data protection.
- Incident reporting.
- Safe browsing habits.
- Security policies and procedures.
- --Training Frequency:-- New employees receive security awareness training as part of their onboarding process. Ongoing training is provided at least annually.
- --Training Methods:-- Training methods include:
- Online training modules.
- Classroom training.
- Phishing simulations.
- Security newsletters.
- --Training Records:-- Records of employee training are maintained to demonstrate compliance with this policy.

--7. Compliance and Auditing--

[Company Name] is committed to complying with all applicable laws, regulations, and industry standards, including ISO/IEC 27001.

- --Internal Audits:-- Internal audits are conducted regularly to assess compliance with this policy and identify areas for improvement.
- --External Audits:-- External audits are conducted periodically by qualified auditors to verify compliance with ISO/IEC 27001 and other applicable standards.
- --Policy Review:-- This policy is reviewed and updated at least annually, or more frequently as needed, to adapt to evolving threats and business changes. The review is performed by the IT Department and approved by the Management Team.
- --Documentation:-- All cybersecurity policies, procedures, and controls are documented and maintained.
- --Non-Compliance:-- Violations of this policy may result in disciplinary action, up to and including termination of employment.

--8. Conclusion--

This Cybersecurity Policy is critical to protecting [Company Name]'s information assets and maintaining the trust of our stakeholders. All employees are expected to adhere to this policy and to report any suspected security vulnerabilities or incidents. By working together, we can create a more secure environment for our business and our customers.

This policy is a living document and will be updated periodically to reflect changes in the threat landscape and our business operations. The IT Department is available to answer any questions about this policy.

--Key Improvements Made:--

- --Risk Assessment:-- Clarified the risk assessment methodology (semi-quantitative), roles and responsibilities, how risk appetite/tolerance is determined, and included periodic penetration tests. Addressed the "low-risk environment" assumption by acknowledging its nature and emphasizing proactive controls.

- --Access Control:-- Provided specifics on acceptable password complexity, password change frequency, and the technologies used for multi-factor authentication. Added sections on access logging and monitoring.
- --Incident Response:-- Clearly defined roles and responsibilities within the Incident Response Team (Incident Commander, Communications Officer, Technical Lead, Legal Counsel) and provided specific escalation procedures.
- --ISO/IEC 27001 Alignment:-- Emphasized the alignment with ISO/IEC 27001 throughout the document, including referencing ISO/IEC 27005 for risk assessment and mentioning external audits.
- --Data Protection:-- added DLP to prevent sensitive data leaving the company
- --Clarity and Readability:-- Used clear and professional language suitable for all audiences, from executives to technical staff.

Remember to replace the bracketed placeholders (e.g., `[Company Name]`) with your organization's specific information. Also, review and customize this policy to ensure it aligns with your unique business requirements and legal obligations.