Subject: Security Policy Recommendations for Premium House Lights Inc.

Dear [Manager's Name],

I appreciate the opportunity to contribute to our company's security policy. Below are my key recommendations, covering risk tolerance, vulnerabilities, risk management, security policies, and monitoring approaches to enhance our security posture.

Organization Analysis & Risk Tolerance

- **Moderate Risk Tolerance:** As an e-commerce business handling sensitive customer data, we must adopt a proactive security approach to protect transactions and personal information.
- **Customer Trust & Business Reputation:** Premium House Lights values customer trust, making data security a top priority. Any security breach could damage the company's reputation and erode customer confidence.
- **Key Considerations:** Business continuity, data confidentiality, and compliance with regulations (PIPEDA, PCI DSS).

Key Vulnerabilities & Threats

- **Web Server Exposure:** The production network (10.10.1.0/24) is accessible from the internet, increasing the risk of DDoS attacks, SQL injection, and cross-site scripting (XSS). Misconfigurations in web applications or APIs could also expose sensitive data to attackers.
- **Database & File Server Risks:** Unauthorized access to stored payment details and customer data could lead to data breaches. Poor encryption practices or weak access controls may further amplify this risk.
- **Wi-Fi Security Risks:** The employee VLAN (10.10.5.0/24) could be vulnerable to rogue devices and unauthorized access. Weak Wi-Fi encryption standards (e.g., outdated WEP or WPA1 protocols) could allow attackers to intercept network traffic.
- **Phishing & Social Engineering:** Employees might be targeted to gain access to sensitive systems. Attackers could leverage spear-phishing emails, business email compromise (BEC) scams, or voice phishing (vishing) to manipulate employees into disclosing credentials.
- **Supply Chain Attacks:** Third-party vendors, contractors, or software dependencies could introduce security vulnerabilities. If an attacker compromises a supplier, they may gain access to our systems indirectly.

Recommended Risk Management Framework & Processes

- **NIST Risk Management Framework (RMF):** Align our security practices with the NIST RMF, which provides a structured approach to risk management through key steps:
    a. **Categorize** information systems based on impact levels.

  b. **Select** appropriate security controls from NIST 800-53.
  c. **Implement** security controls and document configurations.
  d. **Assess** security controls through audits and penetration testing.
  e. **Authorize** systems before deployment based on security readiness.
  f. **Monitor** security posture continuously for emerging threats.

- **Risk Assessment Process:** Conduct ongoing risk assessments to identify, analyze, and prioritize security threats using quantitative and qualitative risk analysis techniques.
- **Incident Response Plan:** Establish a clear protocol for handling security incidents, including breach notifications, forensic analysis, and post-incident reviews.
- **Third-Party Risk Management:** Assess and monitor vendors and partners for security compliance, ensuring they meet our security requirements to prevent supply chain attacks.
- **Business Continuity & Disaster Recovery (BC/DR):** Develop and test a BC/DR plan to minimize downtime and ensure rapid recovery in case of cyber incidents or system failures.

Security Policy Recommendations

- **Network Segmentation:**
  a. Restrict access between production and employee VLANs to prevent lateral movement.
  b. Use firewalls and access control lists to enforce least privilege access.
- **Data Protection:**
  a. Encrypt sensitive data at rest and in transit.
  b. Enforce strong authentication and role-based access controls (RBAC).
- **Endpoint Security:**
  a. Deploy antivirus and endpoint detection and response (EDR) solutions.
  b. Ensure all employee devices have up-to-date security patches.
- **Web Security:**
  a. Implement a Web Application Firewall (WAF) to protect against injection attacks.
  b. Regularly update and patch web server software.
- **User Awareness Training:**
  a. Conduct phishing simulations and security awareness programs.
  b. Require employees to use multi-factor authentication (MFA).

Monitoring Indicators of Compromise (IoCs)

- **Intrusion Detection Systems (IDS):** Implement an IDS to monitor for suspicious network activity.
- **Log Analysis & SIEM:** Use a Security Information and Event Management (SIEM) system to analyze logs for potential threats.
- **Anomaly Detection:** Monitor for unusual access patterns, failed login attempts, and data exfiltration attempts.

- **Threat Intelligence Feeds:** Subscribe to threat intelligence services to stay ahead of emerging threats.

Enhancing Security Posture with Regular Assessments

- **Vulnerability Scanning:** Conduct scans bi-weekly to identify security weaknesses.
- **Penetration Testing:** Perform annual penetration tests to assess real-world attack scenarios.
- **Patch Management:** Maintain an updated patching schedule for all software and firmware.
- **Backup Strategy:** Implement automated, encrypted backups with regular recovery tests.

Next Steps

I recommend implementing these measures in phases, prioritizing critical vulnerabilities first. A sample action plan can be found in the attachment. Let me know how you'd like to proceed or if any points need further clarification.

Best regards,
Anastasiya Gruneva
Cyber Security Analyst
Premium House Lights Inc.

Attachment:

Action Plan

Phase 1: Immediate (0-3 Months)

Action Item	Priority	Owner
Implement Network Segmentation (ACLs & Firewalls)	High	IT Security Team
Deploy Web Application Firewall (WAF)	High	IT Security Team
Conduct Employee Security Awareness Training	High	HR & IT Security Team
Enforce Multi-Factor Authentication (MFA)	High	IT Security Team

Phase 2: Short-Term (3-6 Months)

Action Item	Priority	Owner
Implement Intrusion Detection System (IDS)	High	IT Security Team
Perform Regular Vulnerability Scanning	Medium	IT Security Team
Conduct Phishing Simulation Exercises	Medium	IT Security Team
Develop & Test Incident Response Plan	High	IT Security Team

Phase 3: Long-Term (6-12 Months)

Action Item	Priority	Owner
Establish Business Continuity & Disaster Recovery Plan	High	IT & Operations
Assess Third-Party Vendor Security	Medium	IT Security Team
Enhance SIEM Capabilities & Log Monitoring	Medium	IT Security Team
Conduct Annual Penetration Testing	Medium	IT Security Team