# Risk Assessment and Mitigation Plan for Tech Shop

## 1. Risk Assessment

Key Risks for an E-commerce Website:

* Cybersecurity Risks:  
  - Website hacking and customer data breaches.  
  - DDoS attacks causing downtime.  
  - Payment data leaks and fraud.
* Payment Failures:  
  - Payment processing errors or bank rejections.  
  - Fraudulent transactions (e.g., stolen credit cards).
* Performance & Availability Risks:  
  - Slow website loading times affecting user experience.  
  - Server downtime leading to lost sales.
* Inventory Management Risks:  
  - Selling out-of-stock products due to outdated data.  
  - Errors in stock records causing order issues.
* Supplier & Logistics Risks:  
  - Delayed product deliveries harming reputation.  
  - Shipping errors or damaged products.
* Legal & Compliance Risks:  
  - Non-compliance with data protection laws (e.g., GDPR).  
  - Intellectual property rights violations.

## 2. Risk Mitigation

Strategies to Address Each Risk:

|  |  |  |
| --- | --- | --- |
| Risk | Mitigation Strategy | Details |
| Cybersecurity | Mitigation | - Implement SSL encryption for data security. - Enable 2FA for admin accounts. - Regularly update firewalls and security patches. |
| Payment Failures | Mitigation / Transfer | - Use reliable payment gateways (e.g., Stripe, PayPal). - Implement fraud detection systems. |
| Performance & Availability | Mitigation | - Use a fast hosting service with CDN to improve speed. - Implement load balancing to prevent server crashes. |
| Inventory Management | Mitigation | - Sync real-time inventory with ERP to prevent stock issues. - Automate stock updates to avoid errors. |
| Supplier & Logistics | Mitigation / Transfer | - Work with trusted suppliers with contractual agreements. - Offer shipment tracking for customers. |
| Legal & Compliance | Mitigation | - Ensure GDPR and PCI DSS compliance. - Use legal consultants to prevent IP violations. |