Comprehensive Risk Assessment Framework

1. Introduction

This project outlines a risk assessment framework designed for a small Arabic calligraphy business. The aim is to identify potential risks, assess their impact and likelihood, and propose mitigation strategies. The framework will also include relevant policies to enhance the organization's security posture.

2. Business Context

- **Business Name**: Summies Arts
- **Key Activities**: Designing and customizing bags, caps, and clothes with Arabic calligraphy.
- **Assets**: Customer data, digital calligraphy designs, order management systems, and physical equipment.
- **Stakeholders**: Business owners, customers, and suppliers.

3. Risk Register

Risk ID	Description	Category	Likelihood	Impact	Risk Level	Mitigation Plan	Responsible Person
1	Data breach via phishing emails	Cyber	High	High	High	Implement two-factor authentication; conduct phishing awareness training.	Business Owner
2	Equipment failure	Operational	Medium	High	High	Schedule regular maintenance; have backup equipment.	Business Owner
3	Malware infection	Cyber	Medium	High	High	Install antivirus software; update software regularly.	Business Owner
4	Customer data loss	Cyber	Low	High	Medium	Backup customer data weekly to a secure cloud service.	Business Owner
5	Supply chain disruptions	Operational	Medium	Medium	Medium	Maintain multiple suppliers; keep an inventory of	Business Owner

						essential materials.	
6	Insider threats	People	Low	Medium	Low	Implement role-based access controls; monitor employee activities.	Business Owner
7	Power outage	Operational	Medium	Medium	Medium	Use UPS devices; explore backup power options.	Business Owner

4. Risk Assessment Matrix

Likelihood vs. Impact Grid

- **Likelihood**: Low, Medium, High.
- **Impact**: Low, Medium, High.

	Low Impact	**Medium Impact**	**High Impact**
Low	Low Risk	Low Risk	Medium Risk
Medium	Low Risk	Medium Risk	High Risk
High	Medium Risk	High Risk	High Risk

5. Mitigation Plan

High-Priority Risks

1. **Data Breach**:
    - **Mitigation**: Implement multi-factor authentication, conduct regular security training for staff, and use email filtering tools.
    - **Responsible Person**: Business Owner.
2. **Equipment Failure**:
    - **Mitigation**: Establish a maintenance schedule, create a list of trusted repair services, and budget for spare parts.
    - **Responsible Person**: Business Owner.
3. **Malware Infection**:

    - **Mitigation**: Install reputable antivirus software, update all systems regularly, and restrict downloads from unverified sources.
    - **Responsible Person**: Business Owner.

6. Policies

6.1 Data Protection Policy

- **Purpose**: Ensure the secure handling of customer data.
- **Scope**: Applies to all staff and contractors.
- **Guidelines**:
    1. Store customer data on encrypted devices.
    2. Restrict access to customer data to authorized personnel.
    3. Perform weekly backups to a secure cloud service.

6.2 Acceptable Use Policy

- **Purpose**: Define acceptable usage of company devices and networks.
- **Scope**: Applies to all staff and contractors.
- **Guidelines**:
    1. Do not install unauthorized software.
    2. Avoid accessing personal email or social media on company devices.
    3. Report suspicious activity immediately.

7. Conclusion

This risk assessment framework provides a structured approach to identifying, assessing, and mitigating risks for a small business. The inclusion of clear policies ensures that the organization adopts proactive measures to safeguard its operations and assets.