**1. Define Your Business at a High-Level**

**Business Name:** TrendyCommerce

**Business Overview:** TrendyCommerce is an eCommerce platform specializing in trendy fashion, electronics, and home goods. It aims to provide a seamless shopping experience with a wide range of products, fast delivery, and excellent customer service. TrendyCommerce operates primarily online but also has a few flagship stores in major cities for customer pickups and returns.

**Business Model:**

* **B2C (Business to Consumer):** Directly selling products to customers via an online platform.
* **Marketplace:** Allowing third-party sellers to list and sell products on the platform.

**2. Define Your Company's Assets**

**Digital Assets:**

* **Website and Mobile Apps:** The primary sales channels for TrendyCommerce.
* **Product Database:** Catalog of all products, descriptions, prices, and inventory levels.
* **Customer Database:** Personal information, purchase history, and preferences.
* **Transaction Data:** Records of all sales, returns, and exchanges.
* **Marketing Data:** Analytics, customer engagement, and marketing campaign data.

**Physical Assets:**

* **Inventory:** Products stored in warehouses ready for shipping.
* **Warehouses:** Storage facilities for inventory.
* **Office Equipment:** Computers, servers, and other office infrastructure.

**Human Assets:**

* **Employees:** Staff responsible for operations, customer service, IT, and management.
* **Third-Party Sellers:** Vendors who list their products on the platform.

**3. Define Your Possible Threats**

**Cyber Threats:**

* **Data Breaches:** Unauthorized access to customer or company data.
* **DDoS Attacks:** Distributed Denial of Service attacks causing website downtime.
* **Malware/Ransomware:** Malicious software affecting systems and data.

**Operational Threats:**

* **Server Failures:** Hardware or software failures affecting the website or databases.
* **Network Outages:** Internet or network disruptions impacting accessibility.
* **Supply Chain Disruptions:** Delays or interruptions in product supply or delivery.

**Physical Threats:**

* **Natural Disasters:** Events like earthquakes, floods, or fires affecting physical locations.
* **Theft/Vandalism:** Physical theft or damage to company property or warehouses.

**Reputational Threats:**

* **Negative Publicity:** Bad reviews or negative media coverage affecting customer trust.
* **Compliance Violations:** Breaches of legal or regulatory requirements leading to fines or legal action.

**4. Define Your RTO and RPO**

**Recovery Time Objective (RTO):**

* **Critical Systems (e.g., Website, Payment Processing):** 1 hour
* **Important Systems (e.g., Order Management, Customer Support):** 4 hours
* **Non-Critical Systems (e.g., Internal Communication Tools):** 24 hours

**Recovery Point Objective (RPO):**

* **Critical Data (e.g., Transaction Records, Customer Data):** 15 minutes
* **Important Data (e.g., Product Listings, Inventory Data):** 1 hour
* **Non-Critical Data (e.g., Marketing Analytics):** 24 hours

**Recovery Plan**

**Preparation:**

1. **Data Backups:** Regular, automated backups of all critical and important data with secure storage solutions.
2. **Redundancy:** Duplicate servers and systems in geographically separate locations to ensure failover capability.
3. **Cybersecurity Measures:** Robust security protocols including firewalls, encryption, and regular security audits.
4. **Supplier Agreements:** Contracts with multiple suppliers to mitigate supply chain risks.

**Response:**

1. **Incident Response Team:** A dedicated team trained to handle emergencies and system failures.
2. **Communication Plan:** Clear communication channels and protocols for informing employees, customers, and stakeholders.
3. **Disaster Recovery Procedures:** Documented and tested procedures for restoring systems and data.

**Recovery:**

1. **System Restore:** Quickly restore systems from backups to operational status.
2. **Data Integrity Checks:** Ensure restored data is accurate and complete.
3. **Customer Communication:** Transparent communication with customers about the issue and steps taken to resolve it.

**Review:**

1. **Post-Mortem Analysis:** Conduct an analysis of the incident to identify weaknesses and areas for improvement.
2. **Continuous Improvement:** Update the recovery plan and systems based on lessons learned to prevent future occurrences.