**C.1 PESTLE Analysis Table**

**Purpose:**  
Pampered Pets' business environment can be impacted by external factors that are identified and evaluated in the PESTLE Analysis Table, especially in context of digitalization. This analysis considers Political, Economic, Social, Technological, Legal, and Environmental factors and suggests mitigation strategies to manage or minimize the potential impact of these factors.

|  |  |  |
| --- | --- | --- |
| **Factor** | **Description** | **Mitigations** |
| Political | Local government policies, increased taxes, or restrictions could impact physical sales; government incentives for digital transformation may disadvantage outdated businesses. | Diversify and modernize operations with online platforms and updated technology to reduce reliance on physical sales. |
| Economic | Economic downturns could reduce consumer spending and foot traffic; outdated technology maintenance costs could strain profitability. | Enhance resilience with energy-efficient technologies and compliance with data regulations to maintain profitability. |
| Social | Shifting consumer preferences towards online shopping and advanced services could reduce in-store visits and damage reputation. | Prepare for external risks with flexible pricing, digital transformation incentives, and a disaster recovery plan. |
| Technological | Outdated systems put businesses at a competitive disadvantage, leading to inefficiencies, cyber vulnerabilities, and the inability to leverage new technologies. |  |
| Legal | Outdated technology may not meet legal requirements for data protection, exposing the business to penalties; changes in consumer protection laws could require online services. |  |
| Environmental | Environmental issues like natural disasters could disrupt operations; outdated technology is less energy-efficient, leading to higher costs and environmental impact. |  |

**C.2 FMEA Analysis Table**

**Purpose:**  
The purpose of the Failure Modes and Effects Analysis (FMEA) Table is to pinpoint ways things could go wrong in the day to day operations at Pampered Pets when transitioning to a digital setup. The table examines the impacts, reasons behind failures how severe they are, how likely they are to happen and how easily they can be detected. It then calculates a Risk Priority Number (RPN) to rank these risks in order of importance. Recommendations, for managing each identified risk are also provided.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Failure Mode** | **Effect** | **Cause** | **Severity (S)** | **Occurrence (O)** | **Detection (D)** | **RPN (Risk Priority Number)** | **Mitigation** |
| Inaccurate Forecasting | Financial losses from excess inventory holding costs or missed sales opportunities due to stockouts. | Reliance on outdated or manual forecasting methods that fail to account for current market trends and seasonality. | 7 | 7 | 5 | 245 | Implement advanced forecasting tools within an ERP system that account for market trends, seasonality, and historical data to improve accuracy. |
| Supply Chain Disruptions | Delays in receiving supplies result in stockouts and operational slowdowns, affecting customer satisfaction and revenue. | Inadequate logistical planning, failure to anticipate or prepare for external disruptions in the supply chain. | 8 | 6 | 3 | 144 | Develop a resilient supply chain strategy that includes multiple suppliers, geographic diversification, and contingency planning for alternative transportation routes. |

**C.3 Proposed Changes for Digitalization Table**

**Purpose:**  
The Table of Proposed Digitalization Upgrades details the strategies that Pampered Pets intends to introduce to upgrade its business practices and keep up with todays digital focused market trends effectively enhancing productivity and customer satisfaction while prioritizing data protection.

|  |  |
| --- | --- |
| **Proposed Change** | **Details** |
| Implementation of an E-Commerce Platform | Develop and launch an online store to expand market reach and cater to the growing preference for online shopping. Integrate the e-commerce platform with existing inventory management systems to ensure real-time stock updates and seamless order fulfillment. |
| Upgrade to a Modern ERP System | Replace the current basic software with a comprehensive ERP system that includes advanced modules for forecasting, inventory management, and supply chain management. Utilize predictive analytics to enhance inventory management and demand forecasting accuracy. |
| Enhancement of Cybersecurity Measures | Deploy MFA, encryption, and RBAC to protect against cyber threats. Upgrade legacy systems to reduce vulnerabilities and improve resilience against cyberattacks. |
| Adoption of Automated Data Governance Tools | Implement automated tools for data management and governance to ensure compliance with regulations such as GDPR. Introduce real-time monitoring and auditing to maintain data integrity and prevent unauthorized access or modifications. |

**C.4 STRIDE Analysis Table**

**Purpose:**  
The STRIDE Analysis Table helps Pampered Pets pinpoint risks to their digitalization initiatives by applying the STRIDE model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege). This table offers an explanation of each potential threat and suggests ways to avoid or reduce their negative effects.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Description** | **Mitigations** |
| Spoofing | Improper security controls could lead to spoofed internal resources, potentially launching phishing campaigns against employees or customers. | Implement MFA, encrypt data, and enforce RBAC to protect against spoofing. |
| Tampering | Lack of complex identity management and encryption allows unauthorized users to modify data, leading to potential corruption or loss. | Use encryption, data masking, and strict access controls to prevent tampering and information disclosure. |
| Information Disclosure | Poor data governance could result in unauthorized access and exposure of sensitive data, risking non-compliance with regulations like GDPR. | Strengthen data integrity and governance to ensure compliance with regulations and protect against unauthorized access. |
| Denial of Service (DoS) | Cyberattacks could disable POS and data management systems, causing operational downtime. | Deploy DDoS protection, establish system redundancy, and regularly patch systems to prevent DoS attacks. |
| Elevation of Privilege (PrivEsc) | Legacy systems with unpatched vulnerabilities increase the risk of attackers gaining elevated access and full control over critical systems. | Enhance security controls, patch legacy systems, and enforce RBAC to mitigate elevation of privilege risks. |

**C.5 CIA Triad Analysis Table**

**Purpose:**  
The CIA Triad Analysis Table evaluates the risks and mitigation strategies for Confidentiality, Integrity, and Availability (CIA) concerning different components of Pampered Pets' digitalization initiatives. Throughout the process of transformation it is crucial to prioritize maintaining data security and ensuring business continuity at all times.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIA Component** | **Area** | **Risk** | **Mitigation** |
| Confidentiality | E-Commerce Platform | Data breaches exposing customer information. | Implement SSL/TLS encryption, secure payment gateways, and strong access controls. Conduct regular security audits. |
| Confidentiality | ERP System Upgrade | Unauthorized access to business-critical data during and after the system upgrade. | Implement RBAC and MFA, and encrypt data during transfer and storage. |
| Confidentiality | Cybersecurity Enhancement | Phishing attacks leading to compromised credentials. | Conduct regular employee training, enforce MFA, and implement email filtering tools. |
| Confidentiality | Automated Data Governance Tools | Inadequate protection of sensitive customer and business data, leading to compliance failures. | Use encryption, data masking, and access controls to comply with regulations like GDPR. |
| Integrity | E-Commerce Platform | Tampering with customer orders or financial transactions, leading to data corruption or financial loss. | Implement data validation checks, transaction logging, and secure coding practices. Perform regular audits. |
| Integrity | ERP System Upgrade | Data loss or corruption during migration from the old to the new ERP system. | Develop a detailed data migration plan with backups and integrity checks. Perform thorough testing before going live. |
| Integrity | Cybersecurity Enhancement | Insider threats or cyberattacks altering or deleting critical data. | Enforce strict access controls, regularly update and patch systems, and monitor for suspicious activity. |
| Integrity | Automated Data Governance Tools | Automated tools failing to maintain data accuracy, leading to decision-making errors. | Combine automated data integrity checks with manual oversight. Conduct regular audits. |
| Availability | E-Commerce Platform | DDoS attacks could make the online platform unavailable to customers. | Deploy DDoS protection services and a CDN to ensure continuous availability. |
| Availability | ERP System Upgrade | System downtime during migration or after the upgrade, leading to operational disruptions. | Schedule the upgrade during off-peak hours, have a disaster recovery plan, and minimize downtime through testing. |
| Availability | Cybersecurity Enhancement | Security measures like MFA causing account lockouts or delays in system access. | Implement user-friendly MFA, provide training, and establish quick recovery procedures for locked accounts. |
| Availability | Automated Data Governance Tools | Over-reliance on automated tools leading to system failures, affecting data accessibility. | Implement redundant systems and regular testing. Include manual processes as backups. |