Sam & Ella Gourmet Food IT Security Recommendations

A person and person wearing aprons

AI-generated content may be incorrect.

Prepared for: IT Manager, Sam & Ella Gourmet Food  
Prepared by: Sebastian Canales Burke  
Date: 2025-04-29

**Table of Contents**

1. Introduction
2. NIST Cybersecurity Framework 2.0 and Process
3. Govern
4. Identify
5. Protect
6. Detect
7. Respond
8. Recover
9. Analysis of Security Principles
   * Least Privilege
   * Least Common Mechanism
   * Defense in Depth
10. Conclusion

**Introduction**

**Purpose**:  
The purpose of this report is to assess Sam & Ella Gourmet Food’s current IT practices and recommend security improvements to protect company assets, customer data, and business operations.

**Target Audience**:  
This report is intended for the IT Manager, who graduated from Heritage College prior to cybersecurity training, and seeks actionable, professional guidance in implementing modern security practices based on the NIST Cybersecurity Framework 2.0.

**1. NIST Cybersecurity Framework 2.0 and Process**

Explain what the NIST CSF 2.0 is, its relevance for small businesses, and outline the steps we will follow to improve the company's cybersecurity posture.

**2. Govern**

Discuss how clear policies, accountability, and management oversight will be established to protect sensitive data and IT systems.

**3. Identify**

Detail how the organization will identify assets, risks, vulnerabilities, and their impact on business operations, with a focus on protecting customer and employee data.

**4. Protect**

Recommend technical and organizational safeguards to ensure assets are adequately protected (e.g., access controls, encryption, secure development practices).

**5. Detect**

Explain how the company will implement systems to detect cybersecurity events early (e.g., monitoring, alerting systems).

**6. Respond**

Outline how the company should prepare to respond to cybersecurity incidents effectively, including incident response planning and communication protocols.

**7. Recover**

Describe the strategies for restoring operations and services after a cybersecurity event, including backups and disaster recovery planning.

**8. Analysis of Security Principles**

**Least Privilege**

Explain how limiting user permissions helps minimize damage from mistakes or malicious actions.

**Least Common Mechanism**

Explain why reducing shared resources between users enhances security.

**Defense in Depth**

Illustrate how layering multiple security measures (physical, technical, administrative) creates a stronger overall defense.

Include a **matrix/table** summarizing where these principles were applied across the recommendations.

**Conclusion**

Summarize the key benefits Sam & Ella will gain by implementing the recommended IT security practices, including increased customer trust, legal compliance, reduced risk, and stronger operational resilience.

I have read and understood the rubric for Assignment 3. I have ensured that all required components for Milestone 1 are included and aligned with the rubric expectations.