PROTECT MY RESTAURANTS

Data Handling Best Practices

1. **Understand Data Sensitivity**
    - Identify and classify data based on its sensitivity. Personal, financial, and confidential business data require extra protection.
    - Only collect and store the data that is necessary for business operations.
2. **Limit Access to Sensitive Data**
    - Implement role-based access controls to ensure that only authorized personnel have access to sensitive information.
    - Regularly review and update access permissions to reflect changes in roles and responsibilities.
3. **Use Encryption for Data Protection**
    - Encrypt sensitive data both at rest and in transit to prevent unauthorized access.
    - Use strong encryption standards and regularly update encryption keys.
4. **Implement Secure Data Disposal Procedures**
    - Ensure that sensitive data is securely deleted when no longer needed, using methods such as shredding or data wiping.
    - Follow industry standards and legal requirements for data retention and disposal.
5. **Regularly Backup Data**
    - Regularly backup critical data to ensure it can be restored in the event of data loss or a security breach.
    - Store backups securely, preferably in an encrypted format, and test backup recovery processes regularly.
6. **Monitor and Audit Data Access**
    - Regularly monitor access to sensitive data to detect unauthorized access or anomalies.
    - Conduct periodic audits to ensure compliance with data handling policies and identify potential security gaps.