**Data Security Policy for a Small Business**

**1. Purpose and Scope**

This Data Security Policy aligns with widely recognized U.S. federal data protection laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), ensuring compliance with key regulatory standards for safeguarding sensitive data.

The policy is designed to safeguard the confidentiality, integrity, and availability of sensitive data like personal data (PII), financial records, proprietary business information, and any data categorized as confidential. It defines security protocols for protecting data from unauthorized access, disclosure, alteration, and destruction. This policy applies to all employees, contractors, and any system that handles or stores sensitive data.

**Scope:**

This policy applies to small businesses storing, processing, and transmitting sensitive data through on-premise systems, cloud, and third-party services. It encompasses all employees, contractors, and service providers who interact with the business’s data systems, including any third-party vendors that handle business data on behalf of the company.

**2. Roles and Responsibilities**

- **Small Business IT Manager:** Oversees the implementation and enforcement of data security policy, ensuring compliance with HIPAA and GLBA. Manages data breaches and reports incidents in accordance with regulatory guidelines.

**- Data Owners (Small Business Owners or Department Heads**): Define the classification level of business-critical data and ensure appropriate security measures, including compliance with federal laws such as GLBA.

**- Data Custodians (Third-Party Vendors or IT Staff):** Ensure the integrity of business data, manage backups, and implement encryption for secure storage and transmission, following encryption standards required by PCI DSS and other federal guidelines.

- Employees and Contractors: Adhere to this policy by following proper security protocols and reporting suspicious activities or potential data breaches.

**3. Data Classification**

Data is classified based on its sensitivity and the potential impact if exposed, ensuring compliance with federal laws such as HIPAA and GLBA.

**4. Access Control**

In accordance with federal regulations, including the Federal Trade Commission Act (FTC) and the Electronic Communications Privacy Act (ECPA), this policy enforces strict role-based access control (RBAC) and multi-factor authentication (MFA) to protect sensitive communications and data.

**5. Data Encryption**

Data in transit is encrypted using SSL/TLS standards, meeting the Payment Card Industry Data Security Standard (PCI DSS) requirements and the Gramm-Leach-Bliley Act (GLBA), ensuring the confidentiality of financial and personal data.

**6. Data Handling and Transfer**

Sensitive data must only be stored on secure servers or authorized cloud services that meet security standards. All external data transfers must be encrypted and logged in compliance with industry best practices and regulatory standards.

**7. Backup and Recovery**

Full backups of critical systems must be performed regularly, with incremental backups done hourly for key systems. Backups must be stored securely to comply with industry and federal standards.

**8. Incident Response and Reporting**

This policy includes a robust incident response plan, designed in alignment with industry best practices and federal guidelines, ensuring immediate action in case of a data breach to protect business operations and maintain compliance with U.S. data protection laws.

**9. Policy Review and Updates**

This policy must be reviewed annually or whenever regulatory or business environment changes necessitate updates, ensuring ongoing compliance with U.S. data protection laws.