E-Commerce Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

ABC Company continues to enhance the way we provide products and services to our customers. As a convenience to our customers and business partners, we now accept electronic payment via credit cards. following guidelines highlight the most critical issue in providing this service, to ensure that the trusted relationship between ABC Company and its customers is conducted in the most secure, confidential and reliable method possible.

# II. Purpose

This policy ensures that the trusted relationship between ABC Company and its customers is conducted in the most secure, confidential, and reliable method possible.

# III. Scope

This policy applies to all ABC Company Staff that have access to Information Resources.

# IV. Policy

ABC Company Executive Management must review and approve all proposed electronic commerce (e-commerce) solutions. All e-commerce platforms must either be hosted by ABC Company’s IT Department or hosted through a contractual relationship with a third party service provider.

E-commerce solutions will be reviewed based upon the business case, financial impact, technical requirements, and security mechanisms. The associated startup and recurring costs can include, but are not limited to fees for credit card transactions, hosting services or equipment costs, website and database application development and maintenance, customer support, implementing and maintaining merchant equipment, and Accounting Department time to process payments.

All development, maintenance, and support of web applications shall be the responsibility of the IT Department.

E-commerce related data that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure or modification in such a manner to prevent contract dispute and compromise of data.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.03, APO05.03, APO10.05, APO12.02, BAI02.05, BAI04.05, MEA03.01

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(2)

ISO 27001 6.1.2-3, 9.1-2, A.5.1.1, A.8.1, A.8.2.1, A.9, A.10.1, A.12.4

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 AC-1, AC-8, AU-1, CM-1, PA-1, RA-1, SA-1, SC-1, SI-1

NIST Cybersecurity Framework ID.AM-2, ID.AM-6, ID.GV-2, ID.RA-6, PR.AC-7, DE.DP-2

PCI 1.1, 1.3, 1.5, 2.1-3, 2.6, 3.1-2, 3.5, 3.7, 5.1-4, 6.1