Digitech Branding IT Security Policy

(Applicable to the Dynasend Platform)

---

1. Introduction

Digitech Branding (“the Company”) provides the Dynasend email signature management platform. This Information Security Policy establishes the controls and practices used to safeguard customer data, ensure compliance with contractual and regulatory requirements, and maintain trust with customers.

This policy applies to all Company personnel (employees, contractors, and third parties), systems, software, applications, and data environments that create, process, transmit, or store customer or corporate information.

---

2. Governance and Compliance

2.1 System Security Plan (SSP)

The Company maintains a System Security Plan (SSP) that documents the architecture, security responsibilities, technical and administrative safeguards, and operating environment of the Dynasend platform. The SSP is reviewed annually or after significant changes.

2.2 NIST 800-171 Alignment

While formal certification is not feasible due to Company size, the Company aligns its practices with NIST SP 800-171 requirements, including:

- Access control, authentication, and auditing
- Data encryption (in transit and at rest)
- Incident response procedures
- Security awareness training

2.3 Exception Management

Any deviations from established security policies require documented approval by the Chief Security Officer (CSO). Each exception includes risk assessment, compensating controls, and a defined remediation timeline.

2.4 Enterprise Risk Management (ERM)

The Company maintains a lightweight ERM process:

- Annual review of risks to confidentiality, integrity, and availability
- Assignment of risk ownership to leadership
- Tracking of remediation activities
- Documentation of accepted risks

2.5 Regulatory and Contractual Compliance

The Company recognizes that data protection and privacy regulations may apply to customer data depending on the nature of the engagement and the jurisdictions involved.

- Dynasend does not collect or process sensitive personal data (such as financial data, health data, or government identifiers). Customer information handled by the Company is limited to "business card" data — e.g., name, job title, company, business email address, and business phone number — which is considered low-risk in terms of privacy obligations.
- Where applicable, the Company seeks to align with relevant privacy principles such as those outlined in the EU General Data Protection Regulation (GDPR) and US state-level privacy laws, while recognizing that the scope of these laws may not fully apply given the nature of the data collected.
- The Company commits to meeting contractual data handling requirements specified by customers (including restrictions on residency or US-citizen-only access) and to complying with the requirements of the hosting environment, including AWS compliance programs (e.g., SOC 2, FedRAMP).

---

3. Data Classification and Protection

3.1 Data Classification

Information is classified as:

- **Public** – intended for public disclosure
- **Internal** – business-use only
- **Confidential/Customer** – customer data, PII, and proprietary data

3.2 Protection Requirements

- Customer data is encrypted in transit (TLS 1.2/1.3 only) and at rest (AES-256).
- FIPS 140-2 validated cryptographic modules are used where feasible.
- Customer data is not stored on removable media.

3.3 Data Residency and Access Restrictions

- Customer data resides within US-based AWS infrastructure for US and non EU customers. For EU-based customers data resides within EU-based AWS infrastructure.
- Upon request, customer data access will be restricted exclusively to the US citizen CEO.
- The Company can provide an up-to-date inventory of systems storing customer data.

3.4 Data Retention and Destruction

- Customer data is retained only as long as required by contract.
- When deleted, data is destroyed in compliance with NIST 800-88.
- Backup retention periods are configurable; default retention is 30 days.

---

4. Secure Development and Operations

4.1 Patch Management

The Company applies security patches based on severity:

- Critical: within 14 days
- High: within 30 days
- Medium/Low: as part of scheduled maintenance

4.2 Secure Development Life Cycle (SDLC)

- Code is developed with secure coding standards.
- Static code analysis is performed regularly.
- Security testing is integrated into deployment pipelines.

4.3 Configuration and Change Management

Changes to production systems require:

- Formal review and approval
- Testing in non-production environments
- Documented rollback procedures

4.4 Environment Separation

Production and non-production environments are logically separated. Customer production data is not replicated in non-production environments without written consent.

---

5. Access Control and Identity Management

5.1 User Access Controls

- Unique user IDs are required for all personnel.
- Access is granted on the principle of least privilege.
- Multi-factor authentication (MFA) is required for administrative access.
- Access to audit tools is restricted.

5.2 Onboarding and Offboarding

- Access is removed immediately upon employee departure or role change.
- Annual access reviews are performed.

5.3 Security Awareness and Training

- Annual security awareness training is mandatory.
- Targeted training is provided to privileged users (developers, admins).

5.4 Background Checks

- Employees are subject to background verification proportional to job role.
- Contractors with access to sensitive data undergo equivalent screening where feasible.

5.5 Remote Access

Remote access requires VPN, MFA, and encrypted connections.

---

6. Infrastructure and Network Security

6.1 Firewalls and Segmentation

- AWS security groups and network firewalls restrict inbound/outbound traffic.
- Virtual Private Clouds (VPCs) segment management, application, and customer environments.

6.2 Wireless Security

- All wireless access points use WPA2/WPA3 encryption.
- Default credentials are disabled.
- Rogue access points are periodically scanned.

6.3 System Hardening

- Servers follow CIS Benchmarks where applicable.
- Only required ports and services are enabled.
- Antivirus and endpoint protection are deployed.
- AWS Security Hub is used for compliance checks where applicable.

---

7. Monitoring and Testing

7.1 Logging and Monitoring

- System activity and access logs are retained for at least one year.
- Logs are reviewed periodically by the CSO.

7.2 Vulnerability Management

- Vulnerability scans are conducted regularly.
- Identified vulnerabilities are remediated per severity timelines.
- Results are reviewed with leadership.
- AWS Inspector and other AWS-native tools may supplement testing.

7.3 Penetration Testing

- Annual third-party penetration testing is conducted.
- Tests include application and network layers, full infrastructure, and public IPs.
- Results are tracked to remediation closure.

---

8. Incident Response

8.1 Incident Response Plan

- Defines scope, roles, responsibilities, and communications.
- Trained personnel respond to incidents using established playbooks.

8.2 Notification Requirements

- Customers are notified of a confirmed incident within 48 hours.
- Customers will be notified before communication with authorities regarding their data.

8.3 Forensic Readiness

- Evidence (logs, packet captures) is retained for 90 days following an incident.
- Chain-of-custody procedures are followed when preserving evidence.

8.4 Post-Incident Review

- Root cause analysis is performed after each incident.
- Lessons learned are integrated into processes.

---

9. Business Continuity and Disaster Recovery

9.1 Business Continuity Plan (BCP)

- Documented BCP addresses potential service disruptions.
- Reviewed annually and tested at least every 24 months.

9.2 Disaster Recovery Plan (DRP)

- AWS multi-availability zone redundancy is used for high availability.
- In the event of regional failure, services can be restored in a secondary US AWS region.

- Recovery Time Objective (RTO): ≤ 24 hours.
- Recovery Point Objective (RPO): ≤ 24 hours.

9.3 Backup Management

- Automated backups performed daily.
- Backups encrypted and stored in geographically separate US-based AWS regions.
- Backup restoration tested semi-annually.

---

10. Physical and Facilities Security

- Company equipment is secured with locks when not in use.
- Visitors are escorted and access is logged when accessing facilities.
- Devices (laptops, mobiles) use full-disk encryption and strong authentication.
- AWS data centers maintain industry-leading physical security, including perimeter fencing, guards, and multi-factor access control.

---

11. Policy Maintenance and Enforcement

This policy is owned by the Chief Security Officer (currently the CEO).
It is reviewed annually, updated as needed, and distributed to all personnel.

Violations of this policy may result in disciplinary action and/or termination of access.

Conclusion

This IT Security Policy demonstrates Digitech Branding’s commitment to protecting customer information through documented, risk-based, and proportionate controls. The Company balances rigorous security expectations with the operational realities of a small business while meeting the requirements outlined by customers.