A Bastion Intelligence Product
11816 Inwood Rd #3181
Dallas, TX 75244
November 1, 2025

Bastion Intelligence Data Privacy and Security Plan

Provider: Bastion Intelligence (DBA FortaTech Security)

Service: BastionGPT

Effective Date: CY 2025

1.0 Introduction and Scope

This Data Privacy and Security Plan (the "Plan") outlines the policies, procedures, and safeguards that FortaTech Security LLC (DBA Bastion Intelligence) implements to protect Customer Data processed by the BastionGPT service (the "Service").

Bastion Intelligence is committed to protecting the confidentiality, integrity, and availability of all customer data, including Personally Identifiable Information (PII), Protected Health Information (PHI), and data protected by the Family Educational Rights and Privacy Act (FERPA).

Our security program is centered on customer trust, incorporates cybersecurity as a core operational function, and employs a defense-in-depth strategy. This plan describes our alignment with the **NIST Cybersecurity Framework**, the **Health Insurance Portability and Accountability Act (HIPAA)**, and other applicable federal and state regulations.

2.0 Core Security and Compliance Posture

Bastion Intelligence maintains a robust security and compliance posture designed for sensitive data.

- **Certified Infrastructure:** BastionGPT **exclusively operates on HITRUST CSF Certified and SOC 2 Type II attested infrastructure** for all services processing, storing, or transmitting sensitive or confidential customer data. Our infrastructure providers maintain current certifications with annual audits.
- **Company-Level Attestation:** Bastion Intelligence is actively pursuing its own **HITRUST CSF Certification** and **SOC 2 Type II attestation**. We are currently undergoing readiness activities, with no significant technical gaps observed to date.
- **Comprehensive Controls:** In the interim, Bastion Intelligence maintains a comprehensive set of security controls aligned with the HITRUST CSF and HIPAA Security, Privacy, and Breach Notification Rules.

- **Contractual Commitments:** A **HIPAA Business Associate Agreement (BAA)** and a **FERPA Addendum** are incorporated into all applicable customer agreements to provide contractual assurances of our data protection commitments.

3.0 Data Privacy and Security Commitments

This section details how Bastion Intelligence meets and exceeds contractual data protection requirements.

3.1 Compliance with Data Security and Privacy Requirements

Bastion Intelligence ensures all state, federal, and local data security and privacy requirements are met over the life of the contract by:

- **Executing Legal Agreements:** Providing a comprehensive HIPAA BAA and FERPA Addendum as part of the governing Master Services Agreement.
- **Maintaining NIST Alignment:** Adhering to a security program aligned with the NIST Cybersecurity Framework.
- **Continuous Monitoring:** Actively monitoring for changes in federal and state law to ensure the Service remains compliant with all applicable data privacy and security regulations.

3.2 Safeguards for Protected Information

Bastion Intelligence has implemented extensive administrative, technical, and physical safeguards to protect PII, PHI, and all sensitive customer data.

- **Encryption:** Sensitive data is encrypted using industry-standard protocols, such as:
    - **In-Transit:** Transport Layer Security (TLS) 1.2 or higher.
    - **At-Rest:** AES-256 encryption.
- **Internal Access Control:** Access to customer data by Bastion Intelligence personnel is strictly limited according to the **principles of least privilege** and **need-to-know**. Access is restricted to trained individuals for the express purposes of service delivery, abuse monitoring, or resolving technical issues.
- **Authentication:** The Service enforces strong authentication for all users, including:
    - **Multi-Factor Authentication (MFA):** Email-based MFA with adaptive authentication is available on all plans.
    - **Single Sign-On (SSO):** Enterprise plans support integration with the Customer's existing SSO and identity platform.
- **Data Residency:** For customers with a USA billing address, all sensitive data is processed and stored within the United States. Sensitive data from customers with billing addresses in Canada or Australia will reside in their respective country.
- **AI Model Training:** Customer chat and transcription history is **never sold**, **never provided to OpenAI**, and **never used to train or improve AI models**.

3.3 Demonstration of Compliance

Bastion Intelligence demonstrates compliance with security requirements through:

- **Infrastructure Attestation:** Our compliance posture is demonstrated by our exclusive use of infrastructure providers who maintain current **HITRUST CSF Certification** and **SOC 2 Type II attestation**.
- **Third-Party Validation:** We conduct regular internal risk assessments and employ third-party security firms to perform:
    - **Penetration Tests**
    - **Vulnerability Scans**
    - **Security Code Reviews** (performed after every major code modification)
- **Trust and Compliance Portal:** Detailed information on our security and compliance program, including certifications and attestations (as they become available), can be viewed at our Trust Portal: https://fortatech-security.trustshare.com/home
- **Audit Logs:** Audit logs for system access and actions are maintained and monitored by our internal security team and automated security response systems. Applicable logs can be provided to the Customer upon ad-hoc request (subject to terms in the MSA).

3.4 Personnel Training and Awareness

Bastion Intelligence ensures that all personnel who have access to customer data (including PII, PHI, or FERPA-protected data) receive comprehensive training **prior to receiving access**.

- This mandatory training covers all relevant federal and state laws governing data confidentiality, including **HIPAA** and **FERPA**, as well as Bastion's internal data handling policies and security procedures.
- Training is reviewed at least annually and upon any significant change in policy or regulation.

3.5 Subcontractor Management

Bastion Intelligence utilizes a minimal number of subcontractors (third-party vendors) for service delivery.

- **Primary Subcontractor:** Our primary subcontractor is **Microsoft**, which provides the secure, HITRUST-certified cloud infrastructure on which the Service operates.
- **Subcontractor Vetting:** Bastion Intelligence maintains a requisite **HIPAA Business Associate Agreement (BAA)** and other necessary security assurances with Microsoft to ensure all customer data remains protected.
- **Data Access Restrictions:** Apart from authorized contractors, no other third party is granted access to sensitive customer information, PII, or PHI.

3.6 Incident Management and Notification

Bastion Intelligence maintains a documented **Incident Response (IR) Plan** that is regularly reviewed and tested in accordance with industry best practices.

- **Identification:** We utilize a combination of internal monitoring, automated alerts, vulnerability scanning, and code reviews to identify, detect, and analyze potential security incidents.

- **Notification:** In the event of a confirmed Security Incident or Data Breach (as defined in the BAA) implicating PII or PHI, Bastion Intelligence will provide **prompt incident notification** to the Customer. Notification will be made without unreasonable delay and in any event **not to exceed 72 hours** from the time of discovery.

3.7 Data Return, Transition, and Deletion

Upon the termination or expiration of the governing contract, Bastion Intelligence will manage customer data according to the following defined lifecycle:

- **Data Return (Self-Service):** The Customer may use the Service's self-service export features to retrieve and back up their data at any time up to the contract termination or expiration date.
- **Data Transition (Assisted):** Upon request, and for a period of up to **thirty (30) days** past the expiration of the agreement, Bastion Intelligence can share customer records via a secure online file share.
- **Data Deletion and Destruction:** Following this 30-day transition period, all customer data (including PII, PHI, and all chat history) is **permanently deleted (securely wiped)** from production systems in accordance with our data retention schedule.
    - *Note:* Certain metadata or audit logs may be retained for a limited period in secure audit vaults solely to support required auditing and monitoring for illegal or prohibited system use, after which they are also destroyed.

4.0 Contractual Addendums

This Data Privacy and Security Plan is an exhibit to and forms a part of the primary service agreement (e.g., **Master Services Agreement (MSA)** or **Terms of Use**) between Bastion Intelligence and the Customer.

This Plan, the primary agreement, and the public-facing **Privacy Policy** work in conjunction with other specific contractual addendums as applicable to the Customer's data, including:

- **Business Associate Agreement (BAA):** In compliance with 45 C.F.R. Part 160 and Part 164 (HIPAA).
- **FERPA Addendum:** In compliance with 34 C.F.R. § 99.31 (FERPA).