ITS Security Statement

Infrastructure Security

Our application leverages the Firebase system that is part of **Google Cloud Platform (GCP)** for saving application and user data and **Amazon Web Services (AWS)** for hosting the web application and servers that allow integration with Canvas.

Data Protection

- **Encryption in Transit**: All data transmitted between your device and our servers is encrypted using industry-standard **HTTPS and Transport Layer Security (TLS)**. This prevents eavesdropping or tampering with your data as it travels over the internet.
- **Encryption at Rest**: All data stored in **Cloud Firestore** is automatically encrypted at rest by Google using advanced encryption standards (AES-256).

Application & Access Control

Access to user data is controlled through fine-grained rules and authentication mechanisms included in the GCP and AWS cloud services

- **Firestore Security Rules**: The core of our data access control is **Firestore Security Rules**. These are server-side rules that define precisely who can read, write, and query data. By default, access to all data is denied, and we explicitly grant access on a need-to-know basis. This **"deny-all"** default ensures that no data can be accessed unless a rule specifically allows it, preventing unauthorized data exposure.
- **Principle of Least Privilege**: Our internal administrative access to the Firebase project is strictly limited to authorized personnel based on the principle of least privilege, ensuring that only a minimal number of individuals have the credentials to manage the backend infrastructure.
- **CORS**: Access to servers and services storing data is only available to request originating from the its-bhss.org domain.
- **AWS IAM Permissions**: Access to AWS to update and access the web application files and Canvas integration servers only granted to a selected set on personel using IAM roles and policies (similar to Firebase access).