# Threat Model (Light)

**HESA data collection functionality PF**

Date Assessed: 14/05/2025

Prepared by: David Biayna Neal

Reviewed by: Will North, Charlie Harris, Trefor Walters

### Background

People First is being extended to support the production of HESA returns. The process includes enabling HESA, importing data (Person, Contract, Activity, Governor), allowing employees to self-update data, validating data quality, and generating XML exports. Imports can both insert and update records, with overwrites occurring if fields are left blank. There is no versioning or time-effective records — only the latest record per person is retained with a last-updated timestamp. The process aligns with the annual HESA reporting cycle.

### Scope

This threat model focuses on the data handling processes introduced for the HESA return functionality within the People First application. It includes the import mechanisms, user-editable data processes, administrative corrections, and export generation. Interfaces include UI forms, and automated data validations.

### Threat Assessment

The following key threats were identified and assessed.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Mitigation** | **Mitigated** |
| **High:** Personal and sensitive data (e.g. contracts, identifiers) is editable by employees without fine-grained access control, increasing risk of unauthorized or accidental edits. | Role-based access control should be enforced per field and action. Changes should be logged and reviewed. | Only authorized PF roles can access the HESA functionality |
| **Medium:** Manual imports via templates can introduce malformed or inconsistent data. (e.g. invalid codes or identifiers), which may not be detected until XML validation. | Implement strong validation on import templates, with clear feedback on errors and pre-checks before records are committed to the database. | PF only takes specific template when manually imported, it won’t allow any other file type. |

### Conclusion

The implementation is deemed sufficiently secure as only authorized People First user ie certain roles can access the HESA functionality. Furthermore, it will only allow a certain template for the import generated by People First.