# Threat Model (Light)

## Storing historical Itrent Payslip Data

Date Assessed: 28th April 2025

Prepared by: David Biayna Neal

Reviewed by: Will North, Charlie Harris, Trefor Walters

### Background

To improve performance when retrieving iTrent payslips through People First, historical payslip data (which can no longer be changed) will now be stored within the People First platform. Currently, salary and payroll data within People First are not encrypted at rest, and access to the tenant database containing this new data will be managed using existing controls already in place for payroll and salary data. The People First Architecture team was engaged late in the project lifecycle, resulting in a short timeframe before the planned go-live date of April 29, 2025.

### Scope

This threat model assesses whether storing historical iTrent payslip data locally within People First introduces any new threats, with particular focus on encryption at rest requirements.

### Threat Assessment

The following key threats were identified and assessed.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Mitigation** | **Mitigated** |
| **High:** Historical payslip data is stored without encryption at rest, increasing exposure risk in the event of a data breach. | Current payroll and salary data in People First are not encrypted at rest; the same controls (database access controls and auditing) will apply to the historical payslip data. However, encrypting payslip data at rest should be considered for defense-in-depth and future compliance needs. | **No** |

### Conclusion

The Cyber Security team notes that while the design is consistent with existing People First data protection practices, the lack of encryption at rest for historical payslip data remains a residual risk. It is recommended that encrypting payslip data at rest is considered to enhance protection and align with future data protection standards, although this is not a blocker for the planned implementation.