# Threat Model (Light)

**People First Import - PAT Token Role**

Date Assessed: 02/06/2025

Prepared by: David Biayna Neal

Reviewed by: Will North, Charlie Harris, Trefor Walters

### Background

To support automation in onboarding new clients, People First plans to introduce new Personal Access Token (PAT) roles specifically for payroll-related data imports. These roles will allow remote execution of imports, mirroring existing functionality already implemented for HRM, talent, and custom cards. PAT tokens will be scoped by functional area and follow the standard expiration policy (maximum one year).

### Scope

Introduce scoped PAT token roles to enable automated payroll imports in People First, aligned with existing HRM and talent token standards.

### Threat Assessment

The following key threats were identified and assessed.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Mitigation** | **Mitigated** |
| **Medium:** PAT token misuse due to over-permission. | PAT roles are scoped specifically to payroll import functionality. Existing standards for token creation and permission granularity will apply. | Yes |
| **Medium:** PAT token reuse beyond intended purpose or after client decommissioning | PAT tokens expire after max 1 year and can be revoked earlier. | Yes |
| **Medium:** Lateral movement risk if PAT token has access to broader People First functions | Scoping PAT tokens strictly to payroll import APIs should prevent lateral abuse. Existing roles for HRM/talent follow this model. | Yes |

### 

### Conclusion

The introduction of scoped PAT token roles for payroll import automation aligns with existing secure practices already in use within People First. When implemented correctly—adhering to scoping, expiration, secure storage, and revocation protocols—the risk is manageable. However, effectiveness depends on consistent operational discipline around token lifecycle management and audit logging.