Exhibit I

DATAGLYPHIC

DataGlyphic System Security Plan

Note: Last revision: July 18, 2024

The DataGlyphic framework offered by Optina leverages several layers of integration from UKG. DataGlyphic is a proprietary framework designed specifically for UKG. It provides Asynchronous, Anti-Fragile - Management, Monitoring, Altering, Failover and Audit of UKG Data.

The DataGlyphic framework allows for CICD support and integration change. DataGlyphic also extends the capability of the UKG API by enhancing the datapoints and validation available currently.

DataGlyphic System Security Plan

1. Introduction

1. Purpose:

The purpose of this SSP is to outline the security controls and measures implemented to protect HCM and PII data within our platform, ensuring confidentiality, integrity, and availability.

2. Scope:

The scope includes all systems, networks, and data storage mechanisms involved in the processing and management of HCM and PII data.

3. System Identification:

System Name: DataGlyphic Platform, Version: 1.0, Environment: Production

4. Overview:

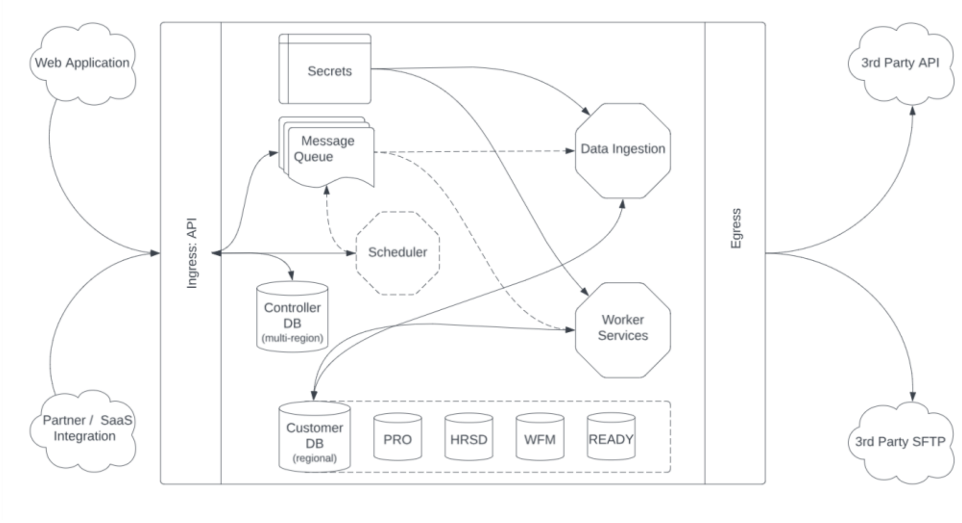
Our system ingests HCM data from various sources, normalizes it into a canonical model, and facilitates data integration and transformation for downstream systems.

2. System Description

1. System Functionality:

Key functionalities include data ingestion, normalization, validation, transformation, and downstream integration.

2. Architecture Diagram:



3. Data Flow Diagram:

Data flows from external systems into our ingestion pipeline where sensitive data is encrypted with each customer's AES256 key. The data is then scrutinized by a series of automated and manual processing steps that validate and transform the data into a canonical model before it is sent downstream via API or file export.

4. System Components and Interfaces:

Main components include secure file transmission, data ingestion services, data transformation services, storage databases, web application, and public API interfaces for data access and integration.

3. Security Controls

1. Access Control:

We use role-based access control (RBAC) and strict authorization policies.

2. Data Security:

Database data and log files are encrypted at rest using MSSQL TDE (AES-256). Customers have a unique AES-256 key that is used for additional field-level encryption of sensitive data, including 3rd party credentials. All ingress and egress traffic must be sent via TLS 1.2 or SFTP.

3. Network Security:

Network security, including firewalls and intrusion detection systems (IDS), is managed by our infrastructure provider (e.g., GCP or colocation services). Additionally, we implement network segmentation and conduct regular network security audits.

4. Physical Security:
Our data centers have biometric access controls, surveillance, and 24/7 security personnel.

5. Operational Security:
We use continuous security monitoring, regular security audits, and have an incident response plan in place. Additional measures include patch management, access reviews, data masking and anonymization, backup, and recovery procedures, change management, and employee training and awareness programs.

6. Compliance and Regulatory Requirements:
We comply with GDPR, HIPAA, and other relevant data protection regulations.

7. Security Policies and Procedures:
Policies include security awareness training, acceptable use policy, and regular security reviews. Automated routines disable inactive users. System-generated AES-256 keys and SSH private keys are injected at operational runtime and are not accessible to users.

8. Risk Assessment:
We perform regular threat modeling, vulnerability assessments, and risk mitigation planning. In addition, all code, container images, and virtual environments are scanned regularly via an industry-leading, open-source security scanner.

4. Security Responsibilities

1. Roles and Responsibilities:
Security responsibilities and system administration tasks are assigned to the CTO.

2. Contact Information for Security Personnel:
Ryan J Nacht, ryan@dataglyphic.com

5. System Environment

1. Operating Systems:
All of our systems, services, and managed services reside on LTS Linux-based systems.

2. Database Management Systems:
We use MSSQL for long-term data storage. Redis and MongoDB may be occasionally used transactionally (and ephemerally) where performance may require higher IOPS or dealing with unstructured data.

3. Application Servers:
The web application and public API reside behind Nginx. The database service (MSSQL), caching service (Redis), and file transfer services (SFTP) are hosted on LTS Linux operating systems. All services are containerized and run on Kubernetes (K8s).

4. Third-Party Services:
We currently do not have any third-party build or runtime dependencies.

6. Incident Response Plan

1. Incident Detection and Reporting:
We use SIEM (Security Information and Event Management) tools for detection and alerting.

2. Response Procedures:
Procedures include immediate containment, investigation, remediation, and communication with stakeholders.

3. Post-Incident Analysis:
We perform root cause analysis, document findings, and implement corrective actions to prevent recurrence.

7. Business Continuity and Disaster Recovery Plan

1. Backup and Restore Procedures:
We perform nightly backups, store them geographically separated from our production systems, and regularly test our restore procedures.

2. Disaster Recovery Strategy:
Our disaster recovery strategy involves a "rebuild" plan. With our system model being stateless, recovery requires redeploying the services and restoring customer databases. In the event of a disaster, we will redeploy services and restore the customer data along with necessary configuration changes.

3. Continuity of Operations Plan:
We have a comprehensive continuity plan that includes alternate sites and remote work capabilities.

8. Maintenance and Review

1. Schedule for Security Plan Reviews:
We review our SSP annually and after any significant system changes.

2. Procedures for Updating the SSP:
Updates are made through a formal change management process, involving review and approval from the security and engineering team.

3. Continuous Monitoring Strategies:
We use automated tools for continuous monitoring, regular vulnerability scans, and periodic security assessments. Tools include Grafana for real-time visualization and monitoring, Slack for alerting and notifications, and Trivy for continuous vulnerability scanning.