DataWorks Global Inc

# Compliance Documentation: Security Optimization Initiative

IT Security Department

# Contents

# Introduction

This compliance document summarizes the Security Optimization Initiative for DataWorks Global Inc. It highlights compliance measures taken during each sprint and their alignment with organizational and industry standards.

# Compliance Goals

*Identity & Access Management (IAM):* Secure authentication and authorization controls. Implement IAM configurations aligned with Zero Trust principles.

*Data Protection:* Protect sensitive data using encryption and access controls.

*Network Security:* Ensure secure communications with Network Security Groups, VPN gateways, and more.

*Operations Monitoring:* Enable centralized monitoring to detect and respond to threats effectively.

*Project Governance:* Maintain transparency and align implementation with organizational objectives.

# Compliance Summary by Sprint

### Sprint 1: Planning and Kickoff

Deliverables: Project Charter, Scope Statement, Risk Management Plan, and Communication Plan.

Compliance Alignment: Defined governance structures and responsibilities.

### Sprint 2: Identity and Access Management

Deliverables: Configured Microsoft Entra ID for Multi-Factor Authentication (MFA). Implemented Role-Based Access Control (RBAC).

Compliance Alignment: Secure user authentication and authorization.

### Sprint 3: Network Security

Deliverables: Configured NSGs and ASGs. Set up Virtual Network Peering and VPN Gateways.

Compliance Alignment: Secure network traffic and enforce encrypted connections.

### Sprint 4: Compute, Storage, and Database Security

Deliverables: Encrypted Azure VMs and enabled JIT access. Configured Transparent Data Encryption (TDE) for Azure SQL databases.

Compliance Alignment: Protect sensitive data in transit and at rest.

### Sprint 5: Operations Monitoring

Deliverables: Configured Microsoft Sentinel for centralized monitoring.

Compliance Alignment: Enabled proactive monitoring and automated incident response.

### Sprint 6: Final Security Testing

Deliverables: Conducted User Acceptance Testing (UAT).

Compliance Alignment: Validated security configurations.

## Monitoring and Reporting

*Metrics Monitored*: MFA adoption and incident response automation.

*Dashboard Features*: Real-time compliance tracking.

## Compliance Enhancements

1. Encryption for all sensitive data.
2. Strengthened access controls.
3. Automated incident responses.

## Recommendation for Continuous Improvements

1. Schedule regular audits.
2. Provide advanced training for team members.
3. Develop incident response playbooks.

## Project Closure

The Security Optimization Initiative has successfully achieved its objectives.