BUSINESS CONTINUITY & DISASTER RECOVERY OVERVIEW

Version 1.0

Effective Date: March 9, 2026

1. Purpose

This BC/DR Overview summarizes Blueshift's resilience, continuity, and disaster recovery practices for the IntelliThreat AI Platform and, where applicable, the Managed SOC & XDR Services. It is informational only and does not create contractual commitments beyond those in the PLATFORM MASTER SUBSCRIPTION AGREEMENT, the DATA PROCESSING ADDENDUM – INTELLITHREAT AI PLATFORM, or the MANAGED SOC & XDR SERVICES ADDENDUM.

2. Business Continuity Program

Blueshift maintains a Business Continuity Program designed to ensure continued operation of critical business functions in the event of disruption. Key components include:

- Documented business impact analysis
- Redundant communication channels
- Executivelevel continuity governance
- Annual review and tabletop exercises

3. Disaster Recovery Program

Blueshift maintains a Disaster Recovery ("DR") Program for the IntelliThreat AI Platform and Managed SOC & XDR Services. The DR architecture is designed around multi-region Oracle Cloud Infrastructure (OCI) with automated data replication, health-check-triggered failover routing capability, and infrastructure-as-code (IaC) enabling rapid environment reprovisioning. Key program components include:

- Multiregion cloud infrastructure (OCI)
- Automated backups and replication
- Infrastructureascode deployment
- Recovery runbooks and escalation procedures

3.1 Recovery Objectives

- **RPO:** ≤ 24 hours
- **RTO:** ≤ 24 hours (Nonbinding targets; commercially reasonable efforts only.)

Autonomous Mode: Upon detection of a service-affecting event, the IntelliThreat Autonomous tier's Kill-Switch automatically suspends in-flight Autonomous Actions. Blueshift replicates Autonomous Action audit logs to a secondary OCI region as part of the Autonomous Action execution workflow. Blueshift employs monitoring designed to detect and alert on replication degradation. Tamper-evident audit records are maintained to preserve log integrity regardless of primary-region availability. Customers should re-validate inte-

gration configurations and re-enable Autonomous Mode only after confirming service restoration.

4. Backup & Retention

- Encrypted backups stored in separate OCI regions
- Daily snapshots
- Retention aligned with the DPA and customer configuration

5. Testing

Blueshift performs DR testing at least annually. Testing includes: (a) full failover validation and restoration exercises at least once per calendar year; (b) quarterly tabletop exercises covering representative disruption scenarios including regional cloud outage, ransomware impact, and key-personnel unavailability; and (c) targeted component-level testing following material infrastructure changes. Test results are reviewed by executive governance. Material findings are assigned remediation owners and tracked to closure on a documented timeline.

6. Managed SOC & XDR Services — BC/DR Coverage

The Managed SOC & XDR Services — including SOC analyst workbenches, SIEM infrastructure, alerting pipelines, and case management systems — are hosted on the same multi-region OCI infrastructure described in §3 above and are subject to the same DR Program, recovery objectives, and annual testing cadence. SOC staffing continuity is maintained through geographically distributed analyst coverage and documented escalation paths to alternate personnel in the event primary staff are unavailable. If primary SOC tooling becomes unavailable during a DR event, Blueshift will notify affected customers through its Service Status Page and, where Customer contact information is available, via direct notification to Customer's registered escalation contacts on file, as soon as practicable after the DR event is confirmed. A documented DR customer notification procedure governs this process independently of Blueshift's standard security incident response process.

7. Customer Responsibilities

This BC/DR Overview addresses Blueshift's internal resilience posture. Customers are responsible for maintaining their own business continuity and disaster recovery capabilities within their environments. In connection with the Blueshift relationship, Customers should:

- Maintain current escalation contact information and integration credentials within the IntelliThreat AI Platform, and promptly update such information as personnel or system configurations change.
- Export Customer Data prior to Agreement expiration or termination in accordance with the Data Processing Addendum – IntelliThreat AI Platform §9 (30-day export window).
- Maintain their own BC/DR controls, backup procedures, and incident response capabilities for their internal environments. Blueshift's DR Program covers the Intelli-

Threat AI Platform and Managed SOC & XDR Services only and does not extend to Customer's systems, networks, or data outside the Platform.

- Following any DR event affecting the Platform or integrations, re-validate integration configurations and test automation workflows before re-enabling Autonomous Mode actions in production environments.