CONTOSO ENTERPRISES Compliance & Risk Management INTERNAL AUDIT REPORT

Report Details: Audit ID: AUD-2026-Q1-017 Report Title: Data Privacy Compliance Review Audit Period: October 1 - December 31, 2025 Report Date: January 15, 2026 Classification: CONFIDENTIAL

Audit Team: Lead Auditor: David Park, Compliance Team Lead Auditors: Maria Gonzalez (IT Compliance), James Chen (Legal) Executive Sponsor: Patricia Williams, CTO

Scope: This audit reviewed customer data handling practices across the CRM and Data Analytics teams, covering data collection, storage, processing, transmission, and retention practices against company policies and regulatory requirements (GDPR, CCPA, SOC 2 Type II).

Systems Reviewed: - Salesforce CRM (Production and Staging) - Azure Data Lake (Analytics Pipeline) - Power BI Reporting Platform - Customer Support Ticketing System (Zendesk) - Marketing Automation (HubSpot)

FINDINGS:

Finding 1: CRITICAL RISK Title: Unencrypted PII in Staging Environment Description: 3 databases in the staging environment contain unencrypted Personally Identifiable Information (PII), including customer names, email addresses, phone numbers, and physical addresses. The staging environment uses production data copies without anonymization. Affected Systems: Salesforce Staging DB, Analytics Staging, Test CRM Impact: Potential data breach exposure for approximately 45,000 customer records Remediation Deadline: February 15, 2026 (30 days) Responsible Team: IT Security - Lead: Kevin O'Brien

Finding 2: HIGH RISK Title: Insufficient Access Log Retention Description: Access logs for customer data systems are retained for only 60 days. Company policy and SOC 2 requirements mandate 180-day retention. Previous audit (AUD-2025-Q2-009) flagged this issue; it remains unresolved. Affected Systems: All customer-facing systems Impact: Inability to investigate historical access patterns; SOC 2 non-compliance Remediation Deadline: March 1, 2026 (45 days) Responsible Team: IT Operations - Lead: Lisa Tran

Finding 3: MEDIUM RISK Title: Stale Employee Accounts with Data Access Description: 12 employee accounts remain active 30+ days after departure. These accounts retain access to customer databases and analytics dashboards. Departed employees include 3 from Engineering, 5 from Sales, and 4 from Marketing. Affected Systems: Active Directory, Salesforce, Azure Data Lake Impact: Unauthorized access risk to sensitive customer data Remediation Deadline: January 31, 2026 (immediate) Responsible Team: HR + IT - Leads: Susan Miller (HR), Kevin O'Brien (IT)

Finding 4: LOW RISK Title: Missing Data Processing Agreements Description: 2 out of 8 third-party data processors lack signed Data Processing Agreements

(DPAs). Both vendors were onboarded in Q3 2025. Contracts exist but DPA addendums were not executed. Vendors: CloudMetrics Analytics, DataSync Pro Impact: GDPR non-compliance for EU customer data Remediation Deadline: February 28, 2026 Responsible Team: Legal - Lead: James Chen

RECOMMENDATIONS: 1. Implement data anonymization pipeline for all non-production environments 2. Extend log retention to 180 days across all systems immediately 3. Deploy automated offboarding workflow integrated with Active Directory 4. Execute DPA agreements with CloudMetrics and DataSync within 30 days 5. Schedule quarterly access reviews for all customer data systems 6. Implement data classification labeling across all repositories

OVERALL RISK ASSESSMENT: HIGH Previous Audit Score: 72/100 Current Audit Score: 61/100 (decline due to recurring findings)

Next Scheduled Audit: April 2026 Escalation: If critical findings are not remediated by deadline, escalation to Board Risk Committee is required per policy GRC-2024-003.