# ChatGPT Response

Rating Summary

• Inherent Risk: High — The vendor processes confidential and potentially PI/SPI data (questionnaire sections Privacy 107–134 and Data Security 230–255), operates production workloads in public cloud (Azure) and with a managed cloud provider (Logicworks), and relies on multiple subservice organizations (Azure, Equinix/Logicworks). Business impact appears material based on breadth of services (managed cloud ops, data handling), external integrations, and presence of AI and API exposure.

• Control Effectiveness: Partially Effective (≈65%) — Policies exist (Information Security Policy, Password Guideline, Employee Handbook), and many questionnaire controls are marked “Yes.” However, multiple critical gaps remain across network security, mobile/BYOD, privacy safeguards, device return on termination, vulnerability management (SCA), and logging. Azure/Logicworks SOC 2 Type 2 reports are unqualified with minor exceptions, but they do not remediate the vendor’s own control gaps.

• Residual Risk: High — Using Beaconer matrix: High Inherent + Partially Effective = High.

Control Testing Metrics

• % Control Coverage: ≈65% (based on SOC 2 attestations for subservice providers and the vendor’s questionnaire; substantial “Yes” responses but with notable “No/N/A” in key domains)

• Total Gaps Identified: 14

• Total Critical Gaps: 6

• Residual Risk Calculation Explanation: Inherent risk is High due to processing PI/SPI and critical service reliance on cloud/subservices. Control posture is Partially Effective given multiple High/Medium findings in Access, Network, Mobile, Privacy, and Monitoring. Per Beaconer matrix, Residual Risk remains High.

Subservice reports (strengths/limitations)

• Microsoft Azure SOC 2 Type 2 (Apr 1, 2022–Mar 31, 2023): Unqualified opinion; exceptions included untimely rotation of certain network device passwords, missing break-glass alerting for part of the period, two secrets not rotated timely, quota configs missing for 2 offerings. Overall controls effective.

• Logicworks SOC 2 Type 2 (Feb 1, 2022–Jan 31, 2023): Unqualified opinion; controls effective across Security, Availability, Confidentiality.

Control Testing (Domain Example – Access Control)

Control Question Vendor Response Evidence / Notes

Program approved & communicated Yes Information Security Policy; Employee Handbook; Questionnaire Q33–35

Regular access review for all Yes Q41 “procedure to review access” = Yes; Q42 privileged access reviews = Yes

IDs are auto terminated on last day Yes Q53 “IDs of terminated employees disabled on last day” = Yes (Note: asset return gap at Q71)

Segregation of duties Yes Q52 segregation of duties = Yes

Controls for Corporate Email on personal phones Yes Q65 “controls for users accessing corporate email on mobile devices” = Yes (but MDM/BYOD gaps below)

MFA deployed Yes Q44 MFA deployed = Yes; Q45 MFA for privileged = Yes

Application supports customer SSO Yes Q47 federated ID (SAML/OpenID/SSO) = Yes

Unique IDs required Yes Q48 = Yes

Principle of least privilege Yes Q50 = Yes

Password policy Yes Password Guideline; Q57–60 “min length/complexity; prohibit PIN alone”

Process to request approval for Access Yes Q49 approvals required = Yes

Password sharing prohibited Yes Q56 = Yes

Passwords are salted & hashed at storage No Information Security Policy states AES-256 encrypted at rest for passwords; no evidence of salted hashing for credentials (security best practice is salted hashing, not reversible encryption)

Gap Analysis

Domain Issues Identified Severity (High/Medium/Low) Risk Counter Measure

Access Control No evidence of salted+hashed password storage for auth secrets (AES encryption noted) High Credential compromise could expose reversible passwords Adopt modern password hashing (Argon2id/bcrypt/scrypt with salt), rotate all affected credentials, vault secrets

Access Control System auto-logoff policy not enforced (Q54 = No) Medium Session hijack risk Implement idle timeout and session lock policies across endpoints and critical apps

Asset Management No process to verify return of assets on termination (Q71 = No) Medium Data leakage from unreturned devices Formalize offboarding checklist; track device return; perform remote wipe where applicable

Network Security No published hardening standards for network devices (Q166 = No); insufficient detail in device logs (Q169 = No) High Increased likelihood of misconfig and undetected network attacks Adopt CIS benchmarks; centralize device logging with sufficient detail; periodic config reviews

Network Security Wireless network controls not implemented (Q176 = No) Medium Unauthorized access via Wi‑Fi Implement WPA3-Enterprise, NAC, segmentation, and rogue AP detection

Network Security Remote admin approvals/logging marked N/A (Q180) Medium Gaps in governance of remote admin Define and enforce approved remote admin pathways; log and review sessions (e.g., bastion + session recording)

Mobile/BYOD BYOD not under MDM; no technical enforcement of PIN/encryption/remote wipe (Q284–285 = No) High Data exfiltration via unmanaged mobile endpoints Deploy MDM (Intune/Workspace ONE); enforce MFA, device encryption, screen lock, remote wipe, jailbreak/root detection

Application Security Software composition analysis (SCA) not performed (Q213 = No) High Supply chain vulnerabilities persist Integrate SCA (e.g., Snyk/Dependabot/GitLab SCA) in CI/CD; define remediation SLAs

Application Security Pre‑prod security reviews lack testing procedures (Q207 = No) Medium Undetected vulns reach prod Define AppSec gates (SAST/DAST/SCA) with sign‑offs pre‑prod

API Security Client-managed API access not supported (Q196 = No) Medium Overbroad API exposure Introduce API gateway with per‑client keys/OAuth scopes; rate limiting, logging

Monitoring/Logging Network device logs lack sufficient detail (Q169 = No) Medium Reduced detect/response capability Increase log verbosity; centralize SIEM; define detection use-cases

Privacy/Safeguards Administrative/technical/physical safeguards to protect personal data marked “No” (Q125) High Regulatory non‑compliance (e.g., GDPR/CCPA) Establish and document safeguards (encryption, access controls, DPIAs, DLP, privacy-by-design); perform gap assessment to applicable laws

Third‑Party Risk No remediation reporting for subcontractor issues (Q84 = No); no third‑party inventory based on risk (Q87 = No) Medium Supply chain blind spots Create third‑party inventory with tiering; track subcontractor issues; integrate into vendor risk management

BCP/DR Prod data center tests not included (Q147 = No) Medium Incomplete DR assurance Include prod DC failover tests/simulations; document RTO/RPO results

Password Management Retention of plaintext/unprotected passwords not prohibited (Q61 = No) High Password disclosure risk Document and enforce prohibition; deploy enterprise password manager with audit; disable “remember password” in apps

Additional Observations

• Policies and governance: Information Security Policy (2021) and Password Guideline (2022) are present and reference strong practices (NIST 800-63 passphrases, 14-char min, AES-256/TLS 1.2, MFA). Ensure these policies are tailored to the current organization (some sections appear templated from D3 Security; validate ownership and scope).

• Privacy Policy: Provided policy appears to be SailPoint’s (dated Oct 6, 2023) and not vendor-specific; this does not constitute the vendor’s privacy notice. Action: Publish an organization-specific privacy notice, data map, DSAR process, and data processing terms.

• Network Diagram: Very high-level; lacks segmentation, trust zones, ingress/egress, identity flows, and controls. Action: Produce an updated detailed diagram to support reviews and audits.

Recommended Remediation Roadmap (prioritized)

1. Privacy and Safeguards: Establish documented administrative/technical/physical safeguards; finalize organization-specific privacy notice and DPIA process; map data flows and retention. (High)

2. Identity & Secret Management: Migrate password storage to salted+hashed; rotate credentials; ensure break-glass processes and alerting (learn from Azure SOC 2 exceptions). (High)

3. BYOD/MDM: Enforce MDM with MFA, encryption, and remote wipe for any endpoint accessing corporate email or data. (High)

4. Network Security Baselines: Adopt network device hardening, enable detailed logging, implement wireless controls, and document remote admin procedures. (High)

5. Secure SDLC: Implement SCA in CI/CD; enforce pre‑prod security testing and approvals. (High)

6. Asset Offboarding: Enforce device return and remote wipe at termination; reconcile in asset CMDB. (Medium)

7. Third‑Party Risk: Build third‑party inventory with risk classification; track remediation for subcontractor issues. (Medium)

8. BCP/DR: Include production failover exercises and report outcomes. (Medium)

Notes on Evidence

• SOC 2 Subservice Orgs: Microsoft Azure SOC 2 Type 2; Logicworks SOC 2 Type 2 (strong posture with minor exceptions). These cover cloud platform controls but do not address the vendor’s internal gaps.

• Vendor Questionnaire: Multiple “Yes” responses support existence of controls; however, explicit “No/NA” responses signal material gaps summarized above.

• Policies: Password Guideline (Sept 2022) requires 14 characters and 6‑month user rotation; InfoSec Policy requires 90 days user/30 days admin—harmonize policy requirements and implement technical enforcement.

Final Beaconer Ratings

• Inherent Risk: High — Processes sensitive data; SaaS/API exposure; dependency on Azure/Logicworks; potential high business impact.

• Control Effectiveness: Partially Effective (≈65% coverage) — Policies exist and many controls are in place; however, several critical deficiencies persist across privacy, network security, mobile/endpoint security, and secrets management.

• Residual Risk: High — Per matrix (High Inherent + Partially Effective = High).