

REGULATORY & INTERNAL POLICY ARCHIVE — Inventory Export

Export: 2024-03-01 | Docs from 2021-2024 | CONFIDENTIAL | NOTICE: Contains multiple versions — conflicts under review

GOV-001 AI Governance Framework — NIST AI RMF Mapping

Owner: AI Ethics Committee / Legal | Updated: 2024-01-15 | v1.3 | Status: Active

Maps internal controls to NIST AI RMF 1.0 (Govern/Map/Measure/Manage). Model inventory: ML-001 Pi Screening (High risk, audited Nov 2023), ML-005 Chatbot (Limited risk, NEVER audited).

FLAG: ML-005 never audited — violates own policy. ML-004 audit 9 months overdue. References "EU AI Act draft Dec 2023" which may be outdated.

GOV-002 Employment Classification & Overtime Guidelines

Owner: Legal / People Ops | Updated: 2023-08-01 | v3.1 | Status: Active (pending 2024 DOL update)

FLSA exemption: salary basis + level + duties test. 2020 rule (CURRENT): \$684/wk (\$35,568/yr). 2024 PROPOSED: \$1,128/wk (\$58,656/yr). Titles do NOT determine exemption.

FLAG: Contains 3 salary thresholds (2019/2020/2024 proposed). Internal payroll uses 2020 thresholds. 2024 rule status unknown — doc says "check DOL website."

GOV-003 Vendor Security Assessment Standard

Owner: Security & Compliance | Updated: February 2024 | v2.1 | Status: Active

Tier 1 (critical, handles PII): full questionnaire + SOC 2 + pen test. Tier 2 (internal tools): abbreviated questionnaire. Tier 3 (<\$5K, no data): self-attestation only.

FLAG: Tier 3 "self-attestation only" conflicts with GOV-010 amendment requiring all vendors to complete abbreviated questionnaire. Tracked in Google Sheet — migrating to Vanta Q2 2024.

GOV-004 Access Control Policy

Owner: IT Security | Updated: 09/15/2023 | v2.8 | Status: Active

MFA all users, SSO Okta, min 12 chars. Vendor access expires with contract. Dormant accounts: annual audit >60 days inactive.

FLAG: Archived v2.3 still in doc: "Azure AD, MFA admin-only, 8 chars." GOV-010 supersedes Sections 2 and 4. Three conflicting versions in circulation.

GOV-005 Vendor Onboarding SOP

Owner: Finance / Procurement | Updated: 2024-01-20 | v4.2 | Status: Active

Vendors >\$5K: SOC 2/ISO 27001, \$2M insurance, security review for L3+ data. Under \$5K: skip security + legal review.

FLAG: "Under \$5K skip security" conflicts with GOV-003 Tier 3 self-attestation AND GOV-010 new minimum requirement. Three docs disagree on low-spend vendor process.

GOV-006 Data Handling & Privacy Policy

Owner: Security & Compliance | Updated: November 2021 | v2.0 | Status: Active

L1-L4 classification. Customer PII: 3 yrs then anonymize. Employee records: 7 yrs. Contracts: duration + 5 yrs. Breach: report within 24 hrs.

FLAG: 3+ years old. GOV-008 proposes replacing retention schedule. Still uses pre-GDPR "anonymize" language — GOV-008 says "delete."

GOV-007 Incident Response Playbook

Owner: Security Operations | Updated: January 10th, 2024 | v5.0 | Status: Active — Confidential

SEV-1: 15 min war room. GDPR 72-hr notification. Blameless post-mortem in 5 days. Escalation: Security !' CTO !'

CEO !' Board.

FLAG: Date format inconsistent with all other docs. References "old email chain process" some teams still use.

GOV-008 Data Retention Policy — Proposed Updates

Owner: Compliance Team | Updated: 2024-02-28 | DRAFT | Status: DRAFT — Pending Legal

Customer PII 3!2 yrs DELETE not anonymize. Notification logs 90!30 days. Audit logs NEW 5 yrs (SOX). Vendor contracts +5!+3 yrs.

FLAG: NOT APPROVED. Contradicts GOV-006. Also conflicts with Product spec GOV-009 (90-day logs).

GOV-009 Smart Notification Engine Spec

Owner: Product — Growth Squad | Updated: Aug 8, 2023 | v1.2 DRAFT | Status: DRAFT — 7 months stale

Push + email notifications. Logs retained 90 days. Legal sign-off on consent: asked Aug 2023, no response.

FLAG: Multi-category: part product spec, part compliance (retention, consent). DRAFT 7 months with no owner action. Budget link broken.

GOV-010 Policy Amendment — Access Control & Vendor Mgmt

Owner: CISO Office | Updated: Feb 20, 2024 | FINAL | Status: APPROVED — Effective Mar 1, 2024

MFA ALL accounts (was admin-only in v2.3). Passwords min 14 chars (was 12 in v2.8). Vendor access re-cert every 90 days. ALL vendors must complete abbreviated questionnaire (was self-attestation for Tier 3). Dormant accounts auto-disable >45 days (was 60).

FLAG: Supersedes GOV-004 Sections 2+4 and GOV-003 Tier 3 rule, but those docs NOT YET UPDATED. This memo governs until docs are revised.