**Name: Melvin Baird**

**Project: GRC REPORT**

**Date: 12/8/2025 GAMBILI CORP — INFORMATION SECURITY POLICY (1-PAGE DRAFT)**

Version: 1.0  
Effective date: 12/82025  
Owner: Chief Information Security Officer (CISO)  
Review: Annual or after a material security event

1. Purpose  
   To protect Gambili Corp’s information assets (including customer PII and payment card data), ensure confidentiality, integrity and availability, and maintain compliance with applicable laws and standards (ISO 27001, GDPR, PCI-DSS).
2. Scope  
   Applies to all employees, contractors, consultants, temporary staff, and third-party service providers that create, process, store, transmit or access Gambili information or systems across all Gambili business units and locations.
3. Policy Statements (core requirements)  
   • Data classification — All data must be classified (Public / Internal / Confidential / Restricted). Handling rules are applied according to classification.  
   • Least privilege & access control — Access to systems and data is granted on a need-to-know basis and reviewed regularly. MFA is required for all remote and privileged access.  
   • Data protection — Sensitive data (PII, PAN) must be encrypted at rest and in transit using industry-accepted cryptography; tokenization or PCI-approved controls used for cardholder data.  
   • Secure development & change management — Production changes follow documented change control and testing procedures. Security requirements are integrated into procurement and development lifecycles.  
   • Endpoint & network security — All endpoints must run approved endpoint protection and be configured per the baseline hardening standard; network segmentation is used to isolate critical systems (e.g., payment systems).  
   • Incident response & breach notification — Security incidents must be reported immediately to the Security Team. The Incident Response Plan defines roles, escalation, containment, forensics, and regulatory notification (including GDPR breach timelines).  
   • Vendor security — Third parties must pass due diligence, contractual security clauses, and ongoing monitoring per the Vendor Risk Policy.  
   • Training & awareness — All personnel receive role-based security and privacy training at onboarding and annually.  
   • Monitoring & logging — Critical systems must produce immutable logs; log retention and review align with compliance requirements.  
   • Compliance & audit — Regular internal audits and periodic external assessments confirm compliance with ISO 27001, PCI-DSS, and GDPR.
4. Roles & Responsibilities  
   • Board / Executive: Approve policy, ensure resourcing.  
   • CISO / GRC Team: Policy owner, risk assessments, controls, monitoring, • Data Owners: Classify data, approve access.  
   • IT / Security Operations: Implement controls, patching, logging.  
   • Employees: Follow policy, report incidents
5. • Data Owners: Classify data, approve access.  
   • IT / Security Operations: Implement controls, patching, logging.  
   • Employees: Follow policy, report incidents.
6. Exceptions & Enforcement  
   Any exception requires documented risk acceptance by the CISO and the relevant business owner. Non-compliance may lead to disciplinary action up to termination.
7. References  
   ISO 27001, PCI-DSS, GDPR, Gambili Risk Register, Incident Response Plan, Vendor Risk Policy.

| **Risk ID** | **Risk Description** | **Category** | **Likelihood (L)** | **Impact (I)** | **Risk Score (L×I)** | **Existing Controls** | **Recommended Mitigation Actions** | **Risk Owner** | **Status** | **Review Date** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| R-001 | Phishing attack leading to credential theft | Cybersecurity | Medium (3) | High (4) | 12 | Email filtering, MFA, awareness training | Quarterly phishing simulations, advanced email threat protection | Security Lead | Open | 01-Dec-2025 |
| R-002 | Payment card data breach via third-party payment processor | Vendor / Compliance | High (4) | High (5) | 20 | PCI-DSS certified vendors, contract clauses | Annual PCI-DSS audit of vendors, enforce encryption/tokenization | GRC Manager | Open | 01-Nov-2025 |
| R-003 | Cloud service misconfiguration exposing sensitive customer data | Technology / Compliance | Medium (3) | High (4) | 12 | Cloud security baseline, access control | Quarterly cloud configuration audits, enable automated compliance monitoring | IT Cloud Manager | Open | 15-Dec-2025 |
| R-004 | GDPR non-compliance (failure to meet DSAR deadlines) | Compliance / Legal | Medium (3) | High (4) | 12 | Data mapping, privacy officer assigned | Automate DSAR tracking, periodic privacy training | Data Protection Officer | Open | 10-Jan-2026 |
| R-005 | Fraudulent purchase of digital products | Operational / Fraud | High (4) | Medium (3) | 12 | Fraud detection tool, transaction limits | Machine learning-based fraud detection, vendor fraud checks | Fraud Prevention Lead | Open | 05-Dec-2025 |
| R-006 | Unauthorized privileged access to PII | Cybersecurity | Medium (3) | High (5) | 15 | Role-based access control, MFA | Quarterly access reviews, privileged access monitoring | Security Operations Lead | Open | 20-Dec-2025 |

**Gambili Corp — Vendor Risk Assessment Checklist**

| **Vendor Name** | **Service Provided** | **Risk Tier (Critical/High/Med/Low)** | **PCI-DSS Applicable? (Y/N)** | **GDPR Applicable? (Y/N)** | **Security Certifications (ISO 27001, SOC 2, etc.)** | **Incident Reporting SLA** | **Encryption in Use (Y/N)** | **Access Control Measures** | **Audit/Assessment Date** | **Risk Rating (High/Med/Low)** | **Mitigation Required** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Example: PayFast | Payment Processing | Critical | Y | Y | PCI-DSS, ISO 27001 | 24 hrs | Y | MFA, RBAC | 05-Aug-2025 | High | Annual PCI review |
| Example: CloudHost Inc. | Cloud Hosting | High | N | Y | ISO 27001, SOC 2 | 48 hrs | Y | Network segmentation, MFA | 02-Jul-2025 | Medium | Quarterly config audit |
| Example: Swift Logistics | Logistics Provider | Medium | N | N | None provided | 72 hrs | N | Physical access control only | 10-Jun-2025 | Medium | Vendor awareness training |
| Example: eBook World | Digital Content Supplier | Low | N | Y | GDPR Compliant | 48 hrs | N | User-level access | 12-May-2025 | Low | Add encryption for data in transit |

**Instructions for Use:**

1. Fill in vendor-specific information before onboarding or during periodic reviews.
2. “Risk Tier” should follow your **Vendor Security & Third-Party Risk Policy** classification.
3. Any “No” in encryption, certifications, or access control should be flagged for remediation.
4. High-risk vendors require **annual audits**; medium/low can follow **biennial or triennial** review.

**Gambili Corp — ISO 27001:2022 Compliance Gap Analysis (Simplified)**

| **ISO 27001 Clause / Annex A Control Area** | **Current Status** | **Gap Identified** | **Recommended Action** | **Priority (High/Med/Low)** | **Owner** |
| --- | --- | --- | --- | --- | --- |
| A.5 Information Security Policies | Draft policies exist (ISP, Vendor, Risk) | Policies not yet formally approved by Board | Seek Board approval and publish company-wide | High | CISO |
| A.6 Organization of Information Security | GRC team formed | Roles/responsibilities not documented for all units | Document and communicate responsibilities | Medium | GRC Manager |
| A.8 Asset Management | Basic asset inventory in IT | No classification for non-IT assets | Expand asset inventory to include all information assets | Medium | IT Asset Manager |
| A.9 Access Control | MFA in place for critical systems | No quarterly access reviews | Implement regular access review process | High | Security Ops Lead |
| A.12 Operations Security | Endpoint protection deployed | No centralized logging of all systems | Implement SIEM for centralized log collection | High | IT Security |
| A.15 Supplier Relationships | Vendor risk checklist in place | Not yet applied to all vendors | Roll out assessment to all active vendors | Medium | Vendor Management Lead |
| A.17 Information Security Aspects of Business Continuity | Backup processes exist | No formal business continuity plan tested | Develop and test BCP annually | High | IT DR Coordinator |

**How to Use:**

* “Current Status” is your existing control environment.
* “Gap Identified” highlights where you’re missing full compliance.
* “Recommended Action” drives the remediation plan.
* Priority guides where to allocate resources first

**1. Overview**

Gambili Corp is rapidly expanding its e-commerce operations across Africa, handling sensitive customer PII and payment card data. Regulatory obligations include **ISO 27001:2022**, **PCI-DSS**, and **GDPR**. This report summarizes current top risks, vendor exposure, and compliance gaps, along with recommended mitigation actions.

**2. Top Risks (from Risk Register)**

| **Risk** | **Risk Score** | **Status** | **Key Mitigation** |
| --- | --- | --- | --- |
| Payment card data breach via vendor | 20 (High) | Open | Annual PCI-DSS audits, encryption/tokenization |
| Unauthorized privileged access to PII | 15 (High) | Open | Quarterly access reviews, privileged access monitoring |
| Cloud service misconfiguration | 12 (Medium) | Open | Quarterly cloud audits, automated compliance tools |
| Phishing attacks | 12 (Medium) | Open | Phishing simulations, advanced email filtering |

**3. Vendor Risk Overview**

* **Critical Vendors:** Payment processors, cloud hosting providers.
* **High Risks Identified:** 2 vendors lack current certifications (ISO 27001 / PCI-DSS).
* **Mitigation Plan:** Apply vendor risk checklist to all vendors by Q4 2025; require contractual clauses for incident reporting and encryption.

**4. Compliance Gap Highlights (ISO 27001)**

* Policies approved but **roles/responsibilities documentation** incomplete.
* **Access review process** not yet formalized.
* No tested **Business Continuity Plan**.
* Missing **centralized logging/SIEM** implementation.

**5. Key Recommendations**

1. **Board Approval & Policy Rollout:** Approve and publish the three foundational security policies.
2. **Strengthen Access Controls:** Implement quarterly access reviews for all privileged accounts.
3. **Enhance Vendor Oversight:** Apply due diligence to all vendors, prioritizing those with sensitive data access.
4. **Close Compliance Gaps:** Implement centralized logging, formalize roles, and develop/test BCP.
5. **Ongoing Risk Monitoring:** Quarterly review of high/critical risks with executive updates.

Top of Form

Bottom of Form