**Data Governance Framework**

**DASC 31003 - Project 1**

**Company: ShopSmart Digital  
Team: Jaxon’s Damnation  
Framework Version: 1.0  
Prepared By: Connor Durbin & Ethan Styles  
Date: 10/06/2025  
Last Updated: 10/06/2025**

**Executive Summary**

**This data governance framework establishes policies, procedures, and controls for managing ShopSmart Analytics' customer data in compliance with the California Consumer Privacy Act (CCPA) and the Federal Information Security Modernization Act (FISMA). The framework defines data classification levels, role-based access controls, data integrity and accuracy standards, and continuous audit mechanisms. It ensures the protection of consumer privacy rights under CCPA and the implementation of federal security controls under FISMA, while enabling secure and compliant use of data for business intelligence and market analytics.**

**Governance Objectives**

**Primary Goals**

1. **[Goal 1 - e.g., Ensure CCPA Compliance]** 
   * **Meet all regulatory requirements for CCPA compliance**
   * **Implement feature for individual users to opt out of there data**
2. **[Goal 2 - e.g., Enable Trusted Analytics]** 
   * **Provide clean, validated data for business intelligence**
   * **Ensure data quality meets stakeholder needs**
   * **Support evidence-based decision making**
3. **[Goal 3 - e.g., Protect Data Privacy]** 
   * **Prevent unauthorized access to sensitive information**
   * **Implement appropriate data masking and de-identification**
   * **Minimize data exposure through least-privilege access**

**Success Criteria**

* **100% of PII fields identified and classified**
* **All compliance requirements mapped to controls**
* **Data quality validation rules implemented for critical fields**
* **Role-based access control (RBAC) design documented**
* **Audit logging capabilities defined**

**Data Classification Scheme**

**Classification Levels**

**Level 1: RESTRICTED (Highest Sensitivity)**

* **Definition: Data that if disclosed could cause severe harm to individuals or the organization**
* **Examples: Full SSNs, patient medical record numbers, financial account numbers**
* **Handling Requirements:** 
  + **Encryption at rest and in transit**
  + **Strict access controls (named individuals only)**
  + **Full audit logging of all access**
  + **Cannot be displayed in reports or dashboards**
  + **Must be masked for all non-authorized users**

**Level 2: SENSITIVE (Moderate Sensitivity)**

* **Definition: Data that if disclosed could cause moderate harm or violate regulations**
* **Examples: Diagnoses, treatment information, masked SSNs (last 4 digits), aggregate financial data**
* **Handling Requirements:** 
  + **Encryption at rest**
  + **Role-based access controls**
  + **Audit logging required**
  + **Can be displayed in reports with appropriate access controls**
  + **De-identification required for research purposes**

**Level 3: INTERNAL (Low Sensitivity)**

* **Definition: Data for internal use that doesn't contain PII or sensitive information**
* **Examples: Aggregated statistics (no groups < 5), de-identified operational metrics**
* **Handling Requirements:** 
  + **Standard security controls**
  + **Access available to all employees**
  + **Basic activity logging**
  + **Can be shared internally without restriction**

**Level 4: PUBLIC (No Sensitivity)**

* **Definition: Data approved for public release**
* **Examples: Published research findings, public reports, marketing materials**
* **Handling Requirements:** 
  + **No special controls required**
  + **May be shared externally**

**Data Classification Matrix**

| **Dataset** | **Table/Source** | **Fields** | **Classification** | **Compliance Driver** |
| --- | --- | --- | --- | --- |
| **ShopSmart Data** | **shopsmart\_customer\_interactions** | **interaction\_id, customer\_id** | **RESTRICTED** | **CCPA** |
| **ShopSmart Data** | **shopsmart\_customer\_interactions** | **interaction\_type, rating, sentiment** | **SENSITIVE** | **CCPA** |
| **ShopSmart Data** | **shopsmart\_customer\_interactions** | **interaction\_text** | **SENSITIVE** | **CCPA** |
| **ShopSmart Data** | **shopsmart\_ecommerce\_data** | **session\_id, user\_id** | **RESTRICTED** | **CCPA** |
| **ShopSmart Data** | **shopsmart\_ecommerce\_data** | **action, product\_price, device\_type, conversion\_type** | **SENSITIVE** | **Internal Policy** |
| **ShopSmart Data** | **shopsmart\_point\_of\_sale** | **transaction\_id, store\_location, payment\_method** | **RESTRICTED** | **PCI DSS** |
| **ShopSmart Data** | **shopsmart\_point\_of\_sale** | **product\_name, quantity, unit\_price** | **SENSITIVE** | **Internal Policy** |
| **ShopSmart Data** | **shopsmart\_supply\_chain** | **transaction\_id, vendor\_name** | **SENSITIVE** | **Internal Policy** |
| **ShopSmart Data** | **shopsmart\_supply\_chain** | **product\_description, quantity, unit\_cost, status** | **INTERNAL** | **Internal Policy** |

**Regulatory Compliance Mapping**

**Primary Regulation: CCPA (California Consumer Privacy Act)**

**Regulation Overview:  
The CCPA is a California state law that enhances privacy rights and consumer protection for residents of California. It applies to ShopSmart because the company collects personal data from California-based customers through its e-commerce and interaction platforms.**

**Key Requirements**

**Requirement 1: Consumer Right to Know & Access**

* **Regulation Text: Consumers have the right to request information about the personal data a business collects, uses, discloses, or sells.**
* **Our Implementation:**
  + **All customer-related data fields (e.g., customer\_id, interaction\_text, session\_id) are classified as RESTRICTED or SENSITIVE.**
  + **Data subject access request (DSAR) process documented and operational.**
  + **Identity verification required for access requests.**
* **Controls Implemented:**
  + **Data classification scheme (this document)**
  + **DSAR workflow documented in customer service SOP**
  + **Access control policies prevent unauthorized data retrieval**
* **Verification Method:**
  + **Access request logs**
  + **Internal DSAR response audit trail**
  + **Role-based access audits**

**Requirement 2: Right to Deletion**

* **Regulation Text: Consumers have the right to request deletion of their personal information, with some exceptions.**
* **Our Implementation:**
  + **Deletion requests integrated into customer service portal**
  + **Deletion workflows linked to database and archive layers**
  + **Exceptions logged with justification per CCPA exemptions**
* **Controls Implemented:**
  + **Automated deletion scripts for customer\_id-linked data**
  + **Manual review process for exception handling**
* **Verification Method:**
  + **Request + deletion logs**
  + **Spot audits of deletion outcomes**
  + **Test DSAR simulations**

**Requirement 3: Data Minimization and Purpose Limitation**

* **Regulation Text: Businesses must limit the collection and use of personal data to what is necessary for the stated purpose.**
* **Our Implementation:**
  + **Each field in customer and e-commerce tables reviewed for business necessity**
  + **"Minimum necessary" principle applied to data retention policies**
* **Controls Implemented:**
  + **Data inventory with justification tags**
  + **Periodic data minimization reviews**
* **Verification Method:**
  + **Quarterly field usage reviews**
  + **Data retention policy logs**

| **Regulation** | **Requirement** | **Control Implemented** | **Responsible Role** | **Status** |
| --- | --- | --- | --- | --- |
| **CCPA** | **Consumer Right to Know & Access** | **DSAR (Data Subject Access Request) process with identity verification** | **Compliance Lead** | **Operational** |
| **CCPA** | **Right to Deletion** | **Automated deletion workflows linked to customer service portal** | **Data Pro** | **In Progress** |
| **CCPA** | **Data Minimization & Purpose Limitation** | **Field-level data inventory and justification tagging** | **Governance Specialist** | **In Progress** |
| **PCI DSS** | **Payment Card Data Protection** | **AES-256 encryption for stored card data; tokenization for processing** | **System** |  |

**Data Access Controls**

**Role-Based Access Control (RBAC) Design**

**Access Level 1: SUMMARY (Lowest Privilege)**

* **Who Gets This Access: [e.g., General analysts, operational staff]**
* **What They Can See:** 
  + **Aggregated data only (no individual records)**
  + **Statistics where groups ≥ 5 (statistical disclosure control)**
  + **Masked PII (e.g., last 4 digits of IDs only)**
  + **De-identified datasets**
* **What They Cannot See:** 
  + **Individual-level records**
  + **Full identifiers (SSNs, names, etc.)**
  + **Small group aggregations (n < 5)**
* **Use Cases: [e.g., Creating population health dashboards, operational reporting]**

**Access Level 2: DETAILED (Moderate Privilege)**

* **Who Gets This Access: [e.g., Clinical researchers with IRB approval, quality improvement teams]**
* **What They Can See:** 
  + **Individual records with masked direct identifiers**
  + **Full medical information (diagnoses, treatments)**
  + **Operational details**
  + **Can perform patient-level analysis**
* **What They Cannot See:** 
  + **Full SSNs, full names**
  + **Contact information**
  + **Highly sensitive notes**
* **Use Cases: [e.g., Clinical outcome studies, quality measure calculations]**

**Access Level 3: ENHANCED (Full Privilege)**

* **Who Gets This Access: [e.g., Privacy officers, data governance team, specific authorized administrators]**
* **What They Can See:** 
  + **All data including full identifiers**
  + **Complete audit logs**
  + **System metadata**
* **What They Cannot See: [None - full access with full audit trail]**
* **Use Cases: [e.g., Compliance audits, data quality remediation, patient matching]**
* **Additional Requirements:** 
  + **Signed data use agreement**
  + **Manager approval**
  + **All access logged and reviewed quarterly**

**Access Control Matrix**

| **User Role** | **Access Level** | **Organizational Filter** | **Allowed Operations** | **Approval Required** |
| --- | --- | --- | --- | --- |
| **[Analyst]** | **SUMMARY** | **[All Hospitals]** | **Read, Aggregate** | **[Manager]** |
| **[Researcher]** | **DETAILED** | **[By Study IRB]** | **Read** | **[IRB + Manager]** |
| **[Privacy Officer]** | **ENHANCED** | **[All]** | **Read, Audit** | **[Executive]** |
|  |  |  |  |  |

**Data Masking and De-identification Rules**

**PII Masking Rules**

**Rule 5: [Add more as needed for your datasets]**

* **Original Format:**
* **Masked Format (SUMMARY level):**
* **Masked Format (DETAILED level):**
* **Masked Format (ENHANCED level):**
* **Implementation:**
* **Applies To:**

**Data Quality Standards**

**Data Quality Dimensions**

**1. Accuracy**

* **Definition: Data correctly represents the real-world entity or event**
* **Our Standard: [e.g., ≥95% of records match source validation]**
* **How We Measure: [e.g., Spot checks against source systems, validation rules]**

**2. Completeness**

* **Definition: All required data is present**
* **Our Standard: [e.g., 0% null values for critical fields]**
* **How We Measure: [e.g., Null count checks in profiling]**

**3. Consistency**

* **Definition: Data is uniform across datasets and over time**
* **Our Standard: [e.g., Same format across all tables]**
* **How We Measure: [e.g., Format validation rules, cross-table checks]**

**4. Timeliness**

* **Definition: Data is current and available when needed**
* **Our Standard: [e.g., Data updated within 24 hours of source change]**
* **How We Measure: [e.g., Timestamp comparisons, SLA monitoring]**

**5. Validity**

* **Definition: Data conforms to defined formats and value ranges**
* **Our Standard: [e.g., 100% of records pass defined validation rules]**
* **How We Measure: [e.g., Validation rule execution reports]**

**6. Uniqueness**

* **Definition: No unintended duplicate records**
* **Our Standard: [e.g., <1% duplicate rate on primary key fields]**
* **How We Measure: [e.g., Duplicate detection queries]**
* **Critical Data Elements (CDEs)**

| **Field Name** | **Dataset** | **Quality Requirement** | **Validation Rule** | **Remediation if Failed** |
| --- | --- | --- | --- | --- |
| * **session\_id** | * **shopsmart\_ecommerce\_data** | * **100% complete and traceable** | * **NOT NULL, must follow UUID format** | * **Reject record, alert Data Steward** |
| * **user\_id** | * **shopsmart\_ecommerce\_data** | * **Must match registered customer** | * **Foreign key check against customer\_id** | * **Flag for referential integrity error** |
| * **product\_price** | * **shopsmart\_ecommerce\_data** | * **Must be positive numeric** | * **> 0** | * **Replace with NULL and alert finance QA** |
| * **device\_type** | * **shopsmart\_ecommerce\_data** | * **Must match allowed values** | * **Must be one of {‘mobile’, ‘desktop’, ‘tablet’}** | * **Replace with “unknown”** |
| * **transaction\_id** | * **shopsmart\_point\_of\_sale** | * **100% unique and traceable** | * **NOT NULL, UNIQUE** | * **Reject record, notify Data Engineer** |
| * **payment\_method** | * **shopsmart\_point\_of\_sale** | * **Must match allowed list** | * **Must be one of {‘credit\_card’, ‘cash’, ‘mobile\_pay’}** | * **Replace with “unverified”, flag** |
| * **store\_location** | * **shopsmart\_point\_of\_sale** | * **Must match valid store code** | * **Validate against master store list** | * **Correct via lookup table** |

**Quality Validation Rules**

**Summary of Rules Implemented:**

**ID Format and Uniqueness Validation**

* **Ensures all key identifiers (customer\_id, session\_id, transaction\_id) are unique and non-null across datasets.**
* **Violations trigger data pipeline rejection and alert Data Quality Lead**

**Data Type and Range Validation**

* **rating, product\_price, and quantity must fall within defined numeric ranges.**
* **Rule automatically flags anomalies (e.g., negative prices, excessive quantities).**

**Required Field Completeness Check**

* **Null-value scan for all critical identifiers, timestamps, and financial fields.**
* **Missing data initiates remediation workflow via data quality tracker.**

**Referential Integrity Validation**

* **Validates that all user\_id and customer\_id pairs exist across both interaction and eCommerce datasets.**
* **Ensures consistent key mapping for analytics joins.**

**Controlled Vocabulary Enforcement**

* **Validates categorical fields (interaction\_type, device\_type, payment\_method) against approved domain lists.**

**Timestamp and Date Consistency Check**

* **Verifies that event timestamps follow chronological order (e.g., session start < conversion).**
* **Ensures no future dated transactions exist.**

**Duplicate Detection and Resolution Rule**

* **Detects duplicate customer interaction logs or repeated transaction entries.**
* **Automatic merge or manual review depending on severity.**

**Data Retention and Disposal**

**Retention Requirements**

**By Data Classification:**

| **Classification** | **Retention Period** | **Retention Driver** | **Storage Location** |
| --- | --- | --- | --- |
| **RESTRICTED** | **7 Years** | **CCPA compliance, PCI DSS** | **[Encrypted storage]** |
| **SENSITIVE** | **5 Years** | **Business analytics continuity** | **[Encrypted Standard storage]** |
| **INTERNAL** | **3 years** | **Operational reporting need** | **[Standard storage]** |
| **PUBLIC** | **Indefinite** | **Marketing and public transparency** | **Public repository or CMS** |

**By Dataset:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | **hopsmart\_ecommerce\_data** | **5 years** | **Business analytics and conversion tracking** | **Secure deletion** | | **shopsmart\_point\_of\_sale** | **10 years** | **Financial reporting and tax audit requirements (PCI DSS, SOX)** | **Secure deletion** | |  |  |  |

**Disposal Procedures**

**Secure Deletion Process:**

**Secure Deletion Process:**

**Identify records meeting retention expiration criteria using automated retention script.**

**Generate list of expired records for Governance review.**

**Obtain written approval from Data Steward and Legal Counsel.**

**Execute deletion using NIST SP 800-88 or DoD 5220.22-M compliant methods.**

**Generate Certificate of Destruction and store in compliance repository.**

**Update Audit Log with timestamp, dataset, number of records deleted, and approver.**

**Backup Management:**

**Backups retained for 90 days before expiration.**

**Expired backups are destroyed securely via overwriting and checksum verification.**

**Restoration requires approval from Data Owner or Compliance Lead.**

**Backup restoration events are logged with reason, date, and authorized personnel.**

**Retention Policy Enforcement:**

**Automated retention tagging applied upon data ingestion.**

**Quarterly review ensures expired data is purged as scheduled.**

**Random audits validate that no restricted or sensitive data persists beyond retention period die to turnover.**

**Audit and Monitoring**

**Audit Logging Requirements**

**What We Log:**

* **All data access (user, timestamp, records accessed)**
* **All data modifications (user, timestamp, before/after values)**
* **Access control changes (who granted/revoked what access)**
* **Data quality rule failures**
* **System configuration changes**
* **Failed access attempts**

**Audit Log Retention:**

* **Active logs: [e.g., 1 year online]**
* **Archive logs: [e.g., 7 years offline]**

**Audit Log Protection:**

* **Logs are append-only (cannot be modified)**
* **Separate access controls from data access**
* **Encrypted at rest**
* **Backed up daily**

**Monitoring and Alerting**

**Real-Time Alerts:**

* **Unauthorized access attempts**
* **Bulk data exports (>1000 records)**
* **Access to ENHANCED level data**
* **Validation rule failures >10%**
* **System errors or outages**

**Regular Reviews:**

* **Daily: Failed access attempts**
* **Weekly: Data quality metrics**
* **Monthly: Access patterns and anomalies**
* **Quarterly: Full access log review**
* **Annually: Complete governance framework review**

**Incident Response**

**Data Breach Response:**

1. **Detection: Identify and contain the breach**
2. **Assessment: Determine scope and impact**
3. **Notification: Report to [Privacy Officer, Legal, affected individuals]**
4. **Remediation: Fix vulnerabilities, strengthen controls**
5. **Documentation: Complete incident report and lessons learned**

**Incident Reporting:**

* **All suspected breaches reported within [e.g., 1 hour]**
* **Privacy Officer notified immediately**
* **Documentation completed within [e.g., 48 hours]**

**Data Stewardship**

**Roles and Responsibilities**

**Data Owner: [Role - e.g., Chief Data Officer]**

* **Ultimate accountability for data governance**
* **Approves governance policies and standards**
* **Resolves escalated data-related issues**

**Data Steward: [Role - e.g., Product Owner]**

* **Day-to-day governance oversight**
* **Enforces policies and procedures**
* **Coordinates with technical teams**
* **Reports on governance metrics**

**Data Custodian: [Role - e.g., Systems Architect]**

* **Technical implementation of governance controls**
* **Maintains security and access controls**
* **Ensures system availability and backup**
* **Implements audit logging**

**Data Quality Lead: [Role - e.g., Governance Specialist 2]**

* **Defines and monitors quality metrics**
* **Implements validation rules**
* **Investigates quality issues**
* **Recommends improvements**

**Compliance Lead: [Role - e.g., Governance Specialist 1]**

* **Ensures regulatory compliance**
* **Maintains compliance documentation**
* **Conducts compliance assessments**
* **Coordinates with legal/privacy teams**

**Data Users: [All team members]**

* **Follow governance policies**
* **Report data quality issues**
* **Use data only for authorized purposes**
* **Maintain confidentiality**

**Decision Rights Matrix**

| **Decision Type** | **Owner** | **Steward** | **Architect** | **Quality Lead** | **Compliance Lead** |
| --- | --- | --- | --- | --- | --- |
| **Access approval** | **Approve** | **Recommend** | **Implement** |  | **Review** |
| **Classification changes** | **Approve** | **Propose** |  |  | **Review** |
| **Quality standards** | **Approve** | **Propose** |  | **Define** | **Review** |
| **Tool selection** | **Approve** | **Recommend** | **Recommend** |  |  |
| **Policy exceptions** | **Approve** | **Recommend** |  |  | **Assess Risk** |

**Governance Metrics and Reporting**

**Key Performance Indicators (KPIs)**

| **Metric** | **Target** | **Current** | **Trend** | **Owner** |
| --- | --- | --- | --- | --- |
| **% PII fields classified** | **100%** | **[%]** | **[↑/↓/→]** | **[Compliance Lead]** |
| **% records passing validation** | **≥95%** | **[%]** | **[↑/↓/→]** | **[Quality Lead]** |
| **Data quality score** | **≥85/100** | **[score]** | **[↑/↓/→]** | **[Quality Lead]** |
| **Audit log coverage** | **100%** | **[%]** | **[↑/↓/→]** | **[Architect]** |
| **Access control implementation** | **100%** | **[%]** | **[↑/↓/→]** | **[Architect]** |
| **Compliance training completion** | **100%** | **[%]** | **[↑/↓/→]** | **[Compliance Lead]** |

**Reporting Schedule**

**Weekly Dashboard:**

* **Data quality metrics**
* **Validation rule pass rates**
* **Failed access attempts**

**Monthly Report:**

* **Governance KPIs**
* **Quality trends**
* **Access reviews**
* **Incident summary**

**Quarterly Review:**

* **Comprehensive governance assessment**
* **Policy effectiveness review**
* **Compliance status**
* **Improvement recommendations**

**Annual Certification:**

* **Full compliance audit**
* **Risk assessment**
* **Governance framework update**

**Implementation Roadmap**

**Phase 1: Foundation (Week 7 - Current Project)**

* **Define data classification scheme**
* **Map compliance requirements**
* **Design access control framework**
* **Document masking rules**
* **Implement basic validation rules**
* **Create audit logging design**

**Phase 2: Implementation (Week 8 - Current Project)**

* **Implement masking rules in code**
* **Deploy validation rules**
* **Test access controls (conceptual)**
* **Generate compliance documentation**
* **Create monitoring dashboard**

**Phase 3: Enhancement (Project 2 - Future)**

* **Add advanced analytics governance**
* **Implement real-time monitoring**
* **Deploy production access controls**
* **Automate compliance reporting**
* **Integrate with ML governance**

**Phase 4: Optimization (Future State documentation)**

* **Implement data catalog**
* **Deploy metadata management**
* **Automate quality remediation**
* **Integrate with enterprise systems**
* **Continuous improvement program**

**Policy Exceptions Process**

**When Exceptions Are Allowed**

**Exceptions to governance policies may be granted for:**

* **Emergency situations requiring immediate data access**
* **One-time analytical needs with proper justification**
* **System limitations preventing policy enforcement**
* **Research studies with IRB approval**

**Exception Request Process**

1. **Request Submission:** 
   * **Complete exception request form**
   * **Provide business justification**
   * **Specify duration of exception**
   * **Identify affected data and users**
2. **Risk Assessment:** 
   * **Compliance Lead reviews regulatory risk**
   * **Data Steward assesses business impact**
   * **Architect evaluates technical feasibility**
3. **Approval:** 
   * **Standard exceptions: Data Steward approval**
   * **High-risk exceptions: Data Owner approval**
   * **Compliance review required for all**
4. **Implementation:** 
   * **Document compensating controls**
   * **Set expiration date**
   * **Enhanced monitoring during exception period**
5. **Review:** 
   * **Weekly review of active exceptions**
   * **Revoke when no longer needed**
   * **Document lessons learned**

**Exception Log**

| **Request ID** | **Date** | **Requestor** | **Reason** | **Risk Level** | **Approval** | **Expiration** | **Status** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **[EX-001]** | **[Date]** | **[Name]** | **[Reason]** | **[High/Med/Low]** | **[Approver]** | **[Date]** | **[Active/Closed]** |

**Training and Awareness**

**Required Training**

**All Data Users:**

* **Data governance overview (1 hour)**
* **Data classification and handling (30 min)**
* **PII protection requirements (30 min)**
* **Incident reporting procedures (15 min)**
* **Frequency: Annually + upon hire/role change**

**Users with DETAILED Access:**

* **All of above, plus:**
* **Advanced data handling procedures (1 hour)**
* **Specific compliance requirements (HIPAA/SOX/GDPR) (1 hour)**
* **Frequency: Annually + upon access grant**

**Users with ENHANCED Access:**

* **All of above, plus:**
* **Privacy and security in-depth (2 hours)**
* **Audit and investigation procedures (1 hour)**
* **Data breach response (1 hour)**
* **Frequency: Semi-annually**

**Awareness Program**

**Ongoing Communication:**

* **Monthly governance newsletter**
* **Quarterly "lessons learned" sessions**
* **Annual governance week campaign**
* **Policy updates communicated within 48 hours**

**Framework Maintenance**

**Review and Update Schedule**

**Quarterly Review:**

* **Assess KPI trends**
* **Review policy effectiveness**
* **Update based on incidents/near-misses**
* **Incorporate regulatory changes**

**Annual Review:**

* **Comprehensive framework assessment**
* **Stakeholder feedback collection**
* **Benchmark against industry standards**
* **Major version update**

**Triggered Reviews:**

* **New regulations or regulatory guidance**
* **Significant data breaches (internal or industry)**
* **Major system changes**
* **Organizational changes**

**Change Management**

**Governance Framework Changes:**

1. **Identify need for change**
2. **Document proposed change and rationale**
3. **Assess impact on existing controls**
4. **Obtain Data Owner approval**
5. **Update documentation**
6. **Communicate to stakeholders**
7. **Provide training if needed**
8. **Monitor effectiveness**

**Version Control**

| **Version** | **Date** | **Changes** | **Approved By** |
| --- | --- | --- | --- |
| **1.0** | **[Date]** | **Initial framework** | **[Product Owner]** |
| **…** |  |  |  |

**Appendices**

**SOX (Sarbanes-Oxley Act) Overview:**

**SOX mandates accurate financial reporting and data integrity controls for publicly traded companies. For ShopSmart's point-of-sale (POS) systems, SOX ensures all financial transactions are traceable, verifiable, and securely retained, reducing risks of fraud and misrepresentation in financial statements.**

**Key Requirements for Our Company:**

* + **Maintain verifiable transaction records for all sales (POS data).**
  + **Enforce segregation of duties for system access and approval processes.**
  + **Retain financial records for at least 10 years to meet audit readiness.**

**Penalties for Non-Compliance:**

* + **Executives may face fines up to $5 million or imprisonment up to 20 years for intentional misreporting or destruction of audit records.**

**GDPR (General Data Protection Regulation) Overview:**

**GDPR governs how personal data of EU residents is collected, stored, and processed. While ShopSmart operates primarily in the U.S., GDPR principles are adopted as best practices for user consent, data minimization, and transparency, especially in marketing analytics and eCommerce platforms.**

**Key Requirements for Our Company:**

* + **Obtain explicit consent for all personal data collection.**
  + **Allow users to request data deletion or export**
  + **Conduct regular data protection impact assessments (DPIAs).**

**Penalties for Non-Compliance:**

* + **fines**

**SO 27001 (Information Security Management Standard) Overview:**

**ISO 27001 defines international best practices for establishing, implementing, maintaining, and improving an Information Security Management System (ISMS). ShopSmart aligns with ISO 27001 controls to maintain confidentiality, integrity, and availability of all consumer and operational data.**

**Key Requirements for Our Company:**

* + **Define and manage a risk-based ISMS covering all critical systems.**
  + **Conduct internal and external security audits annually.**
  + **Implement continuous monitoring and incident response procedures.**

**Penalties for Non-Compliance:**

* + **Loss of certification, reputational harm, and potential legal exposure for data breaches or security failures.**

**Appendix B: Data Classification Decision Tree**

**START: Do you need to classify this data?**

**↓**

**Contains PII (names, session IDs, user IDs, payment details)?**

* + **YES - RESTRICTED**

**Examples: customer\_id, session\_id, payment\_method, transaction\_id**

**Contains PHI/financial/sensitive info (e.g., price, sentiment, or device data)?**

* + **YES - SENSITIVE**

**Examples: product\_price, device\_type, conversion\_type, product\_name**

**For internal use only (aggregated or anonymized data)?**

* + **YES - INTERNAL**

**Examples: store\_location, unit\_cost, operational metrics**

**Approved for public release (marketing reports, open analytics)?**

* + **YES - PUBLIC**

**Examples: published dashboards, summary trend reports, public KPIsAppendix C: Quick Reference Guide**

**Need to share data?**

**What classification level? - Check the Data Classification Matrix and apply appropriate security controls.**

**Who needs access? - Verify that the recipient’s access level (Summary / Detailed / Enhanced) is approved in the RBAC Matrix.**

**For what purpose? - Confirm a legitimate business or research need aligned with data-use policies.**

**How long? - Apply the correct retention tag and set an expiration date if temporary access is required.**

**Log it. - Record all access or data-sharing events in the governance au**

**Found a data quality issue?**

1. **Document the issue (screenshot/example)**
2. **Assess impact (how many records affected?)**
3. **Report to Data Quality Lead**
4. **Tag in validation rule tracking**

**Suspect a breach?**

1. **Don't delay - report immediately**
2. **Contact Privacy Officer**
3. **Preserve evidence**
4. **Don't discuss publicly**

**Appendix D: Contact Information**

**Governance Team Contacts:**

* **Data Owner: [Name, Email, Phone]**
* **Data Steward: [Name, Email, Phone]**
* **Privacy Officer: [Name, Email, Phone]**
* **Compliance Lead: [Name, Email, Phone]**
* **Quality Lead: [Name, Email, Phone]**

**Emergency Contacts:**

* **Security Incident: [Contact]**
* **Privacy Breach: [Contact]**
* **System Outage: [Contact]**

**Acknowledgments**

**This framework was developed for Jaxon’s Damnation on DASC 31003 Project 1.**

**Contributors:**

**Ethan S, Andrew, Abe, Jaxon, Connor**

**References:**

* **Student Academic Records Data Contract (course example)**
* **Project Brief**
* **[Relevant regulation] Official Documentation**
* **Industry best practices and standards**