Security & Compliance Checklist for Incentive Programs

Introduction & Instructions

Overview

Incentive programs often handle sensitive data—personally identifiable information (PII), payment info, and corporate details. Compliance violations and security lapses can lead to significant reputational and financial damage. According to **Deloitte**, 70% of consumers say they would stop doing business with a company after a data breach. This checklist helps you design or audit your incentive programs with robust security and compliance practices.

Purpose

Ensure incentive and loyalty platforms adhere to data privacy regulations and employ robust security measures.

Benefit

By following this **Security & Compliance Checklist for Incentive Programs**, your organization will proactively minimize data risks and meet critical regulatory standards, building trust with participants and stakeholders. Regularly reviewing each section ensures your incentive initiatives remain secure, compliant, and resilient.

How to Use This Checklist

1. **Work Through Each Section**: Each section addresses a critical area of security and compliance, from data privacy to monitoring.
2. **Complete the Interactive Fields**: Look for instructions like "[TEXT FIELD], [CHECKBOX], [RADIO BUTTONS], [DROPDOWN MENU]."
3. **Iterate & Update**: Security and compliance standards evolve. Revisit this checklist regularly to keep your program up to date.

Risk Assessment & Requirements | **Status:** Not Started

1. **Identify Applicable Regulations**
    - GDPR (EU), CCPA (California), HIPAA (if dealing with health data), PCI DSS (if handling credit card transactions), other local regulations.

    Have you mapped out all applicable regulations for your incentive program?

    ☐ Yes
    ☐ No

2. **Scope of Data & Processes**
    - Determine which data types you collect (name, email, financial details) and how they are stored or transferred.

      List all data points you collect from participants (e.g., PII, transaction history).

3. **Document Risk Factors**
    - Identify high-risk processes (e.g., storing payment info, awarding prepaid cards).

      Describe the top 3 risks associated with your current incentive setup.

Data Protection & Privacy | **Status:** Not Started

1. **Data Collection & Consent**
    - Use clear opt-in forms, privacy notices, and disclaimers for participants.

      Is a consent management process in place for collecting personal data?

      ☐ Yes
      ☐ No

2. **Storage & Encryption**
    - Store sensitive data in encrypted databases; use secure servers or cloud environments (SOC 2, ISO 27001 certified).

      Are all sensitive data fields encrypted at rest?

      ☐ Yes

      ☐ No

- ☐ Plan to Implement

3. **Retention & Deletion Policies**
    - Define how long you retain participant data and have a process for deletion upon request.

      Describe your data retention timeline and deletion policy.

4. **Privacy Policy Updates**
    - Ensure your public-facing privacy policy covers your incentive program data use and adheres to the latest regulations.

      Have you updated your privacy policy in the last 12 months?

      - ☐ Yes
      - ☐ No

Access Control & Identity Management | **Status:** Not Started

1. **Role-Based Access**
    - Grant only necessary privileges to employees and vendors (principle of least privilege).

      Do you use role-based access control (RBAC) for the incentive platform?

      - ☐ Yes
      - ☐ No

2. **Multi-Factor Authentication (MFA)**
    - Require MFA for administrators, program managers, and any user with access to sensitive data.

      Is MFA enabled for all admin-level accounts?

      - ☐ Yes
      - ☐ No
      - ☐ Partial

3. **Password Policies**
    - Enforce strong passwords, periodic resets, and account lockouts after multiple failed logins.

      Are password complexity requirements enforced?

      ☐ Yes
      ☐ No

4. **Audit Trails & Logging**
    - Maintain logs of all administrative actions, data exports, and system changes.

      Describe your process for reviewing and storing audit logs.

Vendor & Third-Party Compliance | **Status:** Not Started

1. **Vendor Assessment**
    - Verify that third-party reward providers (e.g., gift card platforms, payment processors) meet security and compliance standards.

      Have you reviewed security documentation from all vendors?

      ☐ Yes
      ☐ No

2. **Service-Level Agreements (SLAs)**
    - Include data protection clauses in contracts with vendors; define breach notification protocols.

      List key SLAs or contractual obligations you require from vendors (e.g., data breach reporting within X hours).

3. **Ongoing Vendor Monitoring**
    - Schedule periodic reviews or audits of third-party systems and processes.

      Do you conduct vendor security audits at least annually?

      ☐ Yes
      ☐ No
      ☐ Plan to Implement

Regulatory Documentation & Reporting | **Status:** Not Started

1. **Compliance Documentation**
    - Maintain updated records: data flow diagrams, GDPR/CCPA compliance checklists, PCI-DSS self-assessments, etc.

      Do you maintain documented proof of compliance (e.g., DPIAs, self-assessments)?

      ☐ Yes
      ☐ No

2. **Incident Response Plan (IRP)**
    - Outline steps for containing and reporting data breaches or security incidents; identify responsible stakeholders.

      Provide a brief summary of your incident response plan (who, what, when, how).

3. **Breach Notification Process**

- Comply with required timelines and communication protocols (e.g., 72-hour reporting for GDPR).

  Does your IRP outline breach notification processes per regulatory requirements?

  - ☐ Yes
  - ☐ No

Implementation & Monitoring | **Status:** Not Started

1. **Deployment Best Practices**
   - Test your incentive platform in a staging environment; conduct pen testing before launch.

     Have you conducted vulnerability scans or penetration tests prior to going live?

     - ☐ Yes
     - ☐ No

2. **Employee & Participant Training**
   - Provide ongoing training for staff on data handling, phishing awareness, and compliance updates.

     Describe how you train employees (e.g., annual security training, monthly bulletins).

3. **Key Security Controls**
   - Firewalls, intrusion detection, anomaly detection, and regular patching cycles.

     Are critical security controls (e.g., IDS/IPS, patch management) in place?

     - ☐ Yes
     - ☐ No
     - ☐ Partially

4. **Regular Audits**
   - Schedule audits (internal or external) to confirm continued adherence to security policies and regulatory guidelines.

Have you defined a routine schedule for internal audits (quarterly, bi-annually)?

- ☐ Yes
- ☐ No

Final Review & Action Plan | **Status:** Not Started

1. **Checklist Completion Status**
   [CHECKLIST] – "Mark each section's status:"
   - Completed
   - In Progress
   - Not Started
2. **Action Items & Timelines**
   - List priority tasks (e.g., encrypting certain data fields, implementing MFA) and their deadlines.

   Outline your next steps for addressing any uncovered gaps or risks.

3. **Stakeholder Sign-Off**
   - Secure approvals from compliance teams, CIO, or legal counsel.

   Compliance & Security Approval

Signature 1: _____

Signature 2: _____