Data Classification and Access Control Policy

TechFlow Solutions, Inc.
Policy Number: TS-SEC-003
Effective Date: January 1, 2024
Last Revised: December 15, 2023
Policy Owner: Sarah Chen, Chief Information Security Officer

---

1. PURPOSE AND SCOPE

This policy establishes data classification levels, access control procedures, and data handling requirements for TechFlow Solutions. It applies to all employees, contractors, and third parties who access company or customer data across our customer analytics platform serving enterprise clients in retail, healthcare, and finance.

2. DATA CLASSIFICATION LEVELS

2.1 Public Data

Definition: Information intended for public consumption with no restriction on distribution

Examples: - Marketing materials and website content - Press releases and public announcements - Job postings and general company information - Published research and whitepapers

Handling Requirements: - No special protection required - Can be shared freely without approval - Standard backup and retention applies - May be stored on public cloud services

Labeling: [PUBLIC] - Green classification label

2.2 Internal Data

Definition: Information intended for internal use that could cause minor harm if disclosed

Examples: - Internal policies and procedures - Employee directories and org charts - Meeting notes and project documentation - Internal training materials - Non-sensitive financial information

Handling Requirements: - Accessible to all employees by default - Should not be shared with external parties without approval - Basic encryption for storage and transmission - Standard access controls apply

Labeling: [INTERNAL] - Yellow classification label

2.3 Confidential Data

Definition: Sensitive information that could cause significant harm to the company if disclosed

Examples: - Customer contracts and pricing information - Proprietary algorithms and source code - Strategic business plans and competitive analysis - Employee personal information and compensation - Financial statements and projections - Security policies and infrastructure details

Handling Requirements: - Access restricted to employees with legitimate business need - Encryption required for storage and transmission - Digital Rights Management (DRM) for document protection - Formal approval required for external sharing - Enhanced audit logging and monitoring

Labeling: [CONFIDENTIAL] - Orange classification label

2.4 Restricted Data

Definition: Highly sensitive information requiring the highest level of protection

Examples: - Customer personally identifiable information (PII) - Protected health information (PHI) for healthcare clients - Financial account information and payment data - Social Security numbers and government IDs - Biometric data and authentication credentials - Legal documents under attorney-client privilege - Security vulnerabilities and incident details

Handling Requirements: - Strict need-to-know access only - Multi-factor authentication required for access - End-to-end encryption for all handling - Air-gapped systems for processing when required - Executive approval required for any external sharing - Continuous monitoring and real-time alerting - Special handling for international data transfers

Labeling: [RESTRICTED] - Red classification label

3. ACCESS APPROVAL WORKFLOWS

3.1 Role-Based Access Control (RBAC) Framework

Standard Role Categories:

Executive Level: - Access: All data classifications with business justification - Approval Authority: Can approve Confidential data access for direct reports - Restrictions: Restricted data access requires CISO approval - Review Cycle: Quarterly access review and certification

Management Level: - Access: Public, Internal, and Confidential data within department - Approval Authority: Can approve Internal data access for team members - Restrictions: Cross-department Confidential data requires director approval - Review Cycle: Semi-annual access review

Senior Individual Contributors: - Access: Public, Internal, and role-specific Confidential data - Approval Authority: None (cannot approve access for others) - Restrictions: Confidential data access requires manager approval - Review Cycle: Annual access review

Standard Employees: - Access: Public and Internal data, limited Confidential data - Approval Authority: None - Restrictions: Any Confidential data requires manager approval - Review Cycle: Annual access review

Contractors and Vendors: - Access: Public data and specifically approved Internal data only - Approval Authority: None - Restrictions: Any non-Public data requires formal approval process - Review Cycle: Contract-specific, maximum annual

3.2 Access Request Process

Standard Access Request (Internal/Confidential Data):

1. **Employee Submission:**
   - Submit request via ServiceNow Access Management portal
   - Business justification required (minimum 100 characters)
   - Specify data categories and systems needed
   - Estimated duration of access requirement
2. **Manager Review (Within 2 Business Days):**
   - Verify business need and role appropriateness
   - Confirm employee has completed required training
   - Approve, reject, or request additional information
   - Option to set automatic expiration date
3. **Security Review (Confidential Data Only):**
   - Automated security clearance check
   - Background verification status confirmation
   - Risk assessment based on data sensitivity
   - CISO notification for high-risk access requests
4. **Provisioning (Within 4 Hours of Approval):**
   - Automatic account provisioning via identity management system
   - Access granted with principle of least privilege
   - User notification with access details and restrictions
   - Training reminder if specialized training required

Restricted Data Access Request:

1. **Formal Request Submission:**
   - Detailed business case with executive sponsorship
   - Specific data elements and use case description
   - Duration and scope limitations
   - Proposed safeguards and handling procedures
2. **Multi-Level Approval:**
   - Direct manager approval

- Department director approval
- CISO security review and approval
- Legal review for compliance implications

3. **Enhanced Security Measures:**
   - Dedicated secure workstation provisioning
   - Additional background check if required
   - Signed data handling agreement
   - Specialized training completion verification
4. **Continuous Monitoring:**
   - Real-time access monitoring and logging
   - Weekly access pattern analysis
   - Immediate alerting for unusual activity
   - Monthly review with security team

3.3 Emergency Access Procedures

Emergency Access Criteria: - Customer-impacting incidents requiring immediate data access - Security incidents requiring forensic investigation - Regulatory requests with legal deadlines - Business continuity situations

Emergency Access Process: 1. **Incident Declaration:** P0 incident declared in ServiceNow 2. **Emergency Authorization:** On-call manager or director approval 3. **Temporary Access:** 24-hour emergency access granted 4. **Retroactive Review:** Full approval process completed within 48 hours 5. **Access Revocation:** Automatic revocation after incident resolution

Emergency Access Monitoring: - All emergency access logged and monitored in real-time - Security team notification within 15 minutes - Executive dashboard showing all active emergency access - Weekly emergency access review and reporting

4. ROLE-BASED PERMISSIONS

4.1 System-Specific Role Definitions

Customer Analytics Platform:

Platform Administrator: - Full system configuration and user management - Access to all customer data and analytics - System performance monitoring and optimization - Security configuration and audit log access - Limited to: Senior Engineering staff (3 employees)

Analytics Manager: - Customer data access for specific assigned accounts - Report creation and dashboard configuration - Limited user management for team members - No access to system configuration or logs - Assigned to: Customer Success Managers (12 employees)

Data Analyst: - Read-only access to anonymized customer data - Pre-built report and dashboard access - No raw data export capabilities - Query logging and

monitoring enabled - Assigned to: Analytics team members (8 employees)

Support Specialist: - Customer account information access (no analytics data) - Ticket creation and tracking capabilities - Limited customer communication tools - No data export or modification capabilities - Assigned to: Customer Support team (6 employees)

Internal Business Systems:

Finance Administrator: - Full access to financial systems and data - Accounts payable and receivable management - Financial reporting and analysis tools - Audit trail access and reporting - Limited to: Finance Director and Senior Accountant (2 employees)

HR Administrator: - Employee personal and compensation information - Benefits administration and reporting - Performance management system access - Legal document access (contracts, agreements) - Limited to: CPO and HR Business Partner (2 employees)

IT Administrator: - System administration across all IT infrastructure - User account management and provisioning - Security tool configuration and monitoring - Backup and disaster recovery systems - Limited to: IT Director and Senior Engineers (4 employees)

4.2 Cross-System Access Matrix

Executive Team Access: - Customer Platform: Analytics Manager level (view-only) - Financial Systems: Read-only access to summary reports - HR Systems: Direct report information only - IT Systems: No direct access (request-based)

Engineering Team Access: - Customer Platform: Platform Administrator for assigned systems - Development Environment: Full access to non-production systems - Production Systems: Read-only with change control process - Security Tools: Limited access based on specialization

Sales Team Access: - Customer Platform: Account-specific Analytics Manager access - CRM System: Full access to assigned accounts and prospects - Proposal System: Access to create and manage sales proposals - Financial System: Read-only access to commission reports

Customer Success Team Access: - Customer Platform: Analytics Manager for assigned accounts - Support System: Full ticket management for assigned customers - Communication Tools: Customer-specific communication channels - Knowledge Base: Full access to customer-facing documentation

4.3 Privilege Escalation and Administrative Access

Temporary Privilege Elevation: - Available for specific tasks requiring elevated access - Maximum duration: 4 hours for standard tasks, 8 hours for

complex projects - Automatic logging and monitoring of all elevated access activities - Manager approval required for any privilege escalation

Administrative Account Management: - Separate administrative accounts for privileged users - Multi-factor authentication required for all administrative access - Administrative sessions automatically terminated after 2 hours of inactivity - Weekly review of all administrative account usage

Emergency Administrative Access: - Break-glass procedures for critical system emergencies - Emergency access automatically expires after 24 hours - Full audit trail and executive notification required - Post-incident review mandatory for all emergency access events

5. DATA RETENTION SCHEDULES

5.1 Customer Data Retention

Customer Analytics Data: - **Retention Period:** 7 years from contract termination - **Business Justification:** Historical analysis and trend identification - **Legal Requirements:** SOX compliance for public company customers - **Data Location:** Primary: AWS US-East-1, Backup: AWS US-West-2 - **Encryption:** AES-256 encryption at rest and in transit

Customer Personal Information: - **Retention Period:** 3 years from last customer interaction - **Legal Basis:** GDPR Article 6(f) legitimate interests - **Right to Erasure:** Customer can request deletion at any time - **Data Minimization:** Automated purging of unnecessary PII elements - **Geographic Restrictions:** EU data stored in EU regions only

Customer Support Records: - **Retention Period:** 5 years from ticket closure - **Business Justification:** Support quality analysis and training - **Sensitive Data:** PII removed after 1 year, technical details retained - **Communication Records:** Email and chat logs included in retention - **Legal Hold:** Extended retention for any legal proceedings

5.2 Employee Data Retention

Personnel Records: - **Active Employees:** Retained throughout employment plus 7 years - **Former Employees:** 7 years from termination date - **Background Checks:** 3 years from completion date - **Performance Reviews:** 5 years from review date - **Training Records:** 7 years to demonstrate compliance

Payroll and Benefits Data: - **Payroll Records:** 7 years per IRS requirements - **Benefits Information:** 6 years after plan year end - **401(k) Records:** Indefinitely per ERISA requirements - **Workers' Compensation:** 30 years for injury claims - **Tax Documents:** 7 years per federal requirements

IT and Security Data: - **Access Logs:** 2 years for standard systems, 7 years for financial systems - **Email Archives:** 7 years for business communications -

Device Usage Logs: 1 year for monitoring and optimization - **Security Incident Records:** 7 years for compliance and analysis - **Training Completion:** 7 years to demonstrate compliance

5.3 Business Data Retention

Financial Records: - **General Ledger:** 7 years per SOX requirements - **Accounts Receivable/Payable:** 7 years - **Tax Records:** 7 years per IRS statute of limitations - **Audit Records:** 10 years for external audit reports - **Insurance Claims:** 7 years from claim resolution

Operational Data: - **Contracts and Agreements:** 7 years after expiration - **Meeting Minutes and Documentation:** 5 years - **Project Documentation:** 3 years after project completion - **Marketing Materials:** 3 years for campaign analysis - **Research and Development:** 10 years for IP protection

Legal and Compliance Data: - **Legal Correspondence:** 10 years - **Regulatory Filings:** 7 years - **Policy Documentation:** 7 years after superseding policy - **Incident Reports:** 7 years - **Compliance Certifications:** 7 years

5.4 Automated Retention Management

Retention Automation Tools: - **Microsoft 365:** Automated retention labels and policies - **Google Workspace:** Data lifecycle management rules - **AWS S3:** Intelligent tiering and lifecycle policies - **Database Systems:** Automated archiving and purging procedures

Retention Monitoring: - **Monthly Reports:** Data retention compliance dashboard - **Quarterly Reviews:** Policy effectiveness and compliance assessment - **Annual Audits:** Comprehensive retention policy audit - **Exception Reporting:** Immediate alerts for retention violations

6. CUSTOMER DATA HANDLING PROCEDURES

6.1 Data Collection and Processing

Data Collection Principles: - **Data Minimization:** Collect only data necessary for stated business purposes - **Purpose Limitation:** Use data only for purposes disclosed to customers - **Consent Management:** Clear opt-in consent for all data collection - **Transparency:** Detailed privacy policy explaining data use

Customer Data Onboarding: - **Data Classification:** Automatic classification during ingestion - **Quality Validation:** Automated data quality checks and validation - **Encryption:** End-to-end encryption during transfer and storage - **Access Provisioning:** Immediate role-based access control application

Processing Limitations: - **Authorized Users Only:** Access limited to employees with legitimate business need - **Purpose Binding:** Data use restricted

to original collection purpose - **Time Limitations:** Processing windows defined by customer contracts - **Geographic Restrictions:** Data processing location restrictions honored

6.2 Data Security and Protection

Technical Safeguards: - **Encryption Standards:** AES-256 for data at rest, TLS 1.3 for data in transit - **Access Controls:** Multi-factor authentication and role-based access - **Network Security:** VPN access required for all remote connections - **Endpoint Protection:** Full disk encryption and endpoint detection

Administrative Safeguards: - **Background Checks:** Comprehensive background verification for data access roles - **Training Requirements:** Annual data privacy and security training mandatory - **Access Reviews:** Quarterly review and certification of data access - **Incident Response:** 24/7 security operations center monitoring

Physical Safeguards: - **Data Center Security:** SOC2-compliant cloud infrastructure providers - **Office Security:** Badge access and visitor management systems - **Device Security:** Full disk encryption and remote wipe capabilities - **Media Handling:** Secure destruction of physical media containing customer data

6.3 Data Sharing and Transfers

Internal Data Sharing: - **Need-to-Know Basis:** Access granted only for specific business functions - **Approval Process:** Manager approval required for cross-department sharing - **Audit Trail:** Complete logging of all data access and sharing activities - **Time Limitations:** Temporary access automatically expires

External Data Sharing: - **Customer Authorization:** Written consent required for any external sharing - **Legal Basis:** Clear legal justification for sharing under GDPR/CCPA - **Data Processing Agreements:** Formal agreements with all data processors - **Transfer Mechanisms:** Standard Contractual Clauses for international transfers

Vendor Data Sharing: - **Vendor Assessment:** Comprehensive security assessment for all data processors - **Contractual Protection:** Data processing agreements with security requirements - **Limited Access:** Vendors receive only minimum necessary data - **Monitoring:** Regular audit of vendor data handling practices

6.4 Customer Rights and Requests

Data Subject Rights (GDPR/CCPA): - **Access Requests:** Customer portal for data access requests - **Rectification:** Process for correcting inaccurate

customer data - **Erasure:** Right to be forgotten implementation - **Portability:** Data export in machine-readable format - **Objection:** Process for customers to object to processing

Request Processing: - **Response Time:** 30 days maximum response time - **Identity Verification:** Secure verification of customer identity - **Impact Assessment:** Evaluation of technical and business impacts - **Documentation:** Complete record of all customer requests and responses

Special Handling: - **Children's Data:** Enhanced protection for users under 16 - **Sensitive Categories:** Special handling for health, financial, and biometric data - **Legal Holds:** Suspension of deletion for legal proceedings - **Regulatory Requests:** Expedited handling for law enforcement requests

7. VIOLATION CONSEQUENCES AND ENFORCEMENT

7.1 Violation Categories and Definitions

Minor Violations: - Accidental sharing of Internal data with unauthorized internal parties - Failure to properly classify data according to guidelines - Missed training deadlines (within 30 days of requirement) - Improper labeling of documents or communications

Consequences: - Verbal counseling and retraining - Written acknowledgment of policy understanding - Enhanced monitoring for 90 days - Mandatory additional training completion

Moderate Violations: - Unauthorized access to Confidential data - Sharing Confidential data without proper approval - Failure to report suspected data breaches within 4 hours - Repeated minor violations within 12-month period

Consequences: - Written warning and formal counseling - Mandatory retraining and certification - Temporary access restrictions - Performance improvement plan initiation

Major Violations: - Unauthorized access to Restricted data - External sharing of Confidential or Restricted data - Intentional circumvention of security controls - Data theft or malicious data handling

Consequences: - Formal disciplinary action up to termination - Legal action and law enforcement notification - Financial liability for damages and remediation - Permanent revocation of elevated access privileges

7.2 Investigation and Disciplinary Process

Initial Investigation (24-48 Hours): 1. **Incident Preservation:** Immediate preservation of evidence and logs 2. **Preliminary Assessment:** Initial scope and impact determination 3. **Stakeholder Notification:** Security team, legal,

and HR notification 4. **Temporary Measures:** Immediate access suspension if warranted

Formal Investigation (5-10 Business Days): 1. **Evidence Collection:** Comprehensive log analysis and documentation 2. **Witness Interviews:** Interviews with relevant employees and witnesses 3. **Impact Assessment:** Full evaluation of data exposure and business impact 4. **Root Cause Analysis:** Identification of underlying causes and control failures

Disciplinary Decision (2-3 Business Days): 1. **Review Committee:** HR, Legal, Security, and Management review 2. **Precedent Analysis:** Consistency with previous disciplinary actions 3. **Mitigation Factors:** Consideration of employee history and cooperation 4. **Final Decision:** Formal disciplinary decision and documentation

Implementation and Follow-up: 1. **Action Implementation:** Execution of disciplinary measures 2. **Process Improvement:** Policy and control updates based on lessons learned 3. **Monitoring:** Enhanced monitoring and follow-up as appropriate 4. **Communication:** Appropriate notification to affected parties

7.3 Legal and Regulatory Consequences

Regulatory Violations: - **GDPR Violations:** Potential fines up to 4% of annual revenue or €20 million - **CCPA Violations:** Civil penalties up to $7,500 per violation - **HIPAA Violations:** Fines ranging from $100 to $1.5 million per incident - **SOX Violations:** Criminal penalties and civil liability

Customer Contractual Violations: - **Service Level Penalties:** Reduced service fees and credits - **Contractual Damages:** Direct and consequential damage liability - **Customer Termination:** Right to terminate for material breaches - **Audit Rights:** Customer audit and inspection rights

Business Impact Consequences: - **Reputation Damage:** Loss of customer trust and market credibility - **Insurance Claims:** Professional liability and cyber insurance implications - **Competitive Disadvantage:** Loss of competitive position in market - **Regulatory Scrutiny:** Increased regulatory oversight and compliance costs

8. DATA GOVERNANCE AND COMPLIANCE

8.1 Data Governance Structure

Data Governance Committee: - **Chair:** Chief Data Officer (Sarah Chen, dual role as CISO) - **Members:** Legal Counsel, Privacy Officer, IT Director, Security Manager - **Meeting Frequency:** Monthly governance meetings, quarterly strategic reviews - **Responsibilities:** Policy development, risk assessment, compliance oversight

Data Stewardship Roles: - **Executive Data Steward:** C-level sponsor for each data domain - **Business Data Stewards:** Department heads responsible

for data quality - **Technical Data Stewards:** IT professionals managing data systems - **Data Custodians:** Day-to-day operational data management

Data Quality Management: - **Quality Metrics:** Accuracy, completeness, consistency, timeliness - **Monitoring Tools:** Automated data quality monitoring and alerting - **Quality Reports:** Monthly data quality scorecards and trend analysis - **Improvement Process:** Continuous improvement based on quality metrics

8.2 Compliance Monitoring and Reporting

Automated Compliance Monitoring: - **Access Pattern Analysis:** AI-powered anomaly detection for unusual access - **Data Loss Prevention:** Real-time monitoring for sensitive data movement - **Classification Compliance:** Automated verification of data classification accuracy - **Retention Compliance:** Automated enforcement of retention schedules

Manual Compliance Reviews: - **Quarterly Access Reviews:** Manager certification of team member access - **Annual Risk Assessments:** Comprehensive review of data risks and controls - **Policy Effectiveness Reviews:** Assessment of policy compliance and effectiveness - **Third-Party Audits:** Annual external audit of data governance practices

Compliance Reporting: - **Executive Dashboard:** Real-time compliance metrics for leadership team - **Regulatory Reports:** Quarterly compliance reports for regulators - **Customer Reports:** Annual transparency reports for customers - **Board Reports:** Quarterly data governance reports to board of directors

8.3 Training and Awareness Programs

Mandatory Training Programs: - **New Employee Orientation:** 4-hour data governance and privacy training - **Annual Refresher Training:** 2-hour update training for all employees - **Role-Specific Training:** Specialized training based on data access level - **Incident Response Training:** Quarterly tabletop exercises and simulations

Training Content and Delivery: - **Interactive Modules:** Engaging online training with knowledge checks - **Real-World Scenarios:** Case studies and practical examples - **Policy Updates:** Regular communication of policy changes and updates - **Certification Programs:** Advanced certification for data stewards

Training Effectiveness Measurement: - **Completion Tracking:** 100% completion rate required for all mandatory training - **Knowledge Assessment:** Regular testing of policy understanding - **Behavioral Metrics:** Measurement of actual behavior change - **Incident Correlation:** Analysis of training effectiveness vs. incident rates

9. CONTACT INFORMATION

9.1 Data Governance Contacts

- **Chief Data Officer:** Sarah Chen, sarah.chen@techflow.com, +1 (415) 987-6543
- **Data Privacy Officer:** Amanda Foster, amanda.foster@techflow.com, +1 (415) 555-5678
- **Data Governance Committee:** data-governance@techflow.com
- **Data Steward Network:** data-stewards@techflow.com

9.2 Access Request Support

- **Access Request Portal:** access.techflow.com
- **Help Desk:** data-access@techflow.com, +1 (415) 555-DATA (3282)
- **Emergency Access:** emergency-access@techflow.com, +1 (415) 555-9999
- **Approval Escalation:** access-escalation@techflow.com

9.3 Compliance and Legal Support

- **Compliance Team:** compliance@techflow.com, +1 (415) 555-COMP (2667)
- **Legal Counsel:** legal@techflow.com, +1 (415) 555-5678
- **Privacy Requests:** privacy@techflow.com, +1 (415) 555-PRIV (7748)
- **Regulatory Affairs:** regulatory@techflow.com

Approved By: - Sarah Chen, Chief Information Security Officer - December 15, 2023 - Amanda Foster, Chief Legal Officer - December 15, 2023 - Jennifer Liu, Chief Technology Officer - December 15, 2023 - David Park, Chief Executive Officer - December 15, 2023

This policy is proprietary and confidential to TechFlow Solutions, Inc.