INFORMATION SECURITY POLICY
Aberdeen Captioning Inc.
DBA: Aberdeen Broadcast Services
Policy Owner: Executive Management
Next Review Date: Annual Review
Document Control:

- Policy Owner: Executive Management
- Classification: Internal Use Only

---

1. PURPOSE AND SCOPE

1.1 Purpose

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of information assets at Aberdeen Captioning Inc. ("Aberdeen," "we," "us," or "our"). This policy ensures that Aberdeen maintains appropriate security controls to protect customer data, business information, and technology infrastructure.

1.2 Scope

This policy applies to:

- All Aberdeen employees, contractors, consultants, and temporary workers
- All information systems, networks, and devices owned or operated by Aberdeen
- All customer data processed by Aberdeen
- All third-party service providers with access to Aberdeen systems or data
- All physical and digital information assets

1.3 Policy Objectives

Aberdeen's information security program is designed to:

- Protect customer data and maintain customer trust
- Comply with applicable laws, regulations, and contractual obligations
- Ensure business continuity and operational resilience
- Prevent unauthorized access, disclosure, modification, or destruction of information
- Maintain the confidentiality, integrity, and availability of information assets

---

2. GOVERNANCE AND LEADERSHIP

2.1 Security Leadership

President: Matthew Cook

- Overall accountability for information security
- Final approval authority for security policies and investments

Executive Vice President: Deepthi Yathiender

- Oversight of security program implementation
- Review and approval of security controls

2.2 IT Security Partner

Aberdeen engages a qualified IT security company to:

- Manage and monitor security infrastructure
- Conduct monthly security and privacy training

- Provide security incident response
- Perform security assessments and updates
- Maintain security tools and technologies

2.3 Roles and Responsibilities

All Employees and Contractors:

- Comply with all security policies and procedures
- Protect assigned credentials and access rights
- Report security incidents immediately
- Complete required security training
- Handle information assets responsibly

Management:

- Enforce security policies within their teams
- Approve access requests for their direct reports
- Ensure team members complete security training
- Support security initiatives and requirements

---

3. INFORMATION CLASSIFICATION

3.1 Data Classification Levels

Aberdeen classifies information into the following categories:

Level 4 (L4) - Restricted/Highly Sensitive:

- Payment card information (PCI data)
- Social Security Numbers
- Financial account numbers
- Government-issued identification numbers
- Protected Health Information (PHI) under HIPAA
- **Aberdeen does not intentionally collect or process L4 data**

Level 3 (L3) - Confidential/Sensitive:

- Customer audio and video content (used only as required for transcription/captioning services)
- Transcripts and captions
- Customer names, addresses, phone numbers, email addresses (used only as required for communication and service delivery)
- Employee personal information
- Proprietary business information
- Client contracts and agreements
- Internal financial records

Level 2 (L2) - Internal Use Only:

- Internal policies and procedures
- Business plans and strategies
- Non-public operational information
- Internal communications

Level 1 (L1) - Public:

- Published marketing materials
- Public website content

- Press releases
- General product information

3.2 Handling Requirements

L3 Confidential/Sensitive Data:

- Encrypted in transit (TLS 1.2+) and at rest (AES 256)
- Access restricted to authorized personnel only
- Must not be shared outside Aberdeen without authorization
- Subject to data retention and deletion policies
- Requires confidentiality agreements for access

L2 Internal Use Only:

- Not to be shared outside the organization
- Protected by access controls
- May be shared internally on need-to-know basis

L1 Public:

- May be freely shared
- Subject to trademark and copyright protections

---

4. ACCESS CONTROL AND AUTHENTICATION

4.1 Access Control Principles

Aberdeen implements access controls based on:

- **Least Privilege:** Users receive minimum access necessary for job functions
- **Need-to-Know:** Access granted only to information required for duties
- **Separation of Duties:** Critical functions divided among multiple individuals
- **Role-Based Access Control (RBAC):** Permissions assigned by job role

4.2 User Authentication

Password Requirements:

- Minimum 12-16 characters in length
- Combination of uppercase, lowercase, numbers, and special characters
- Changed every 90 days
- Cannot reuse previous 5 passwords
- Account lockout after 3 failed login attempts

Multi-Factor Authentication (MFA):

- Required for all remote access to Aberdeen systems
- Required for administrative access to critical systems
- Required for access to Salesforce and AWS infrastructure

4.3 Account Management

User Account Provisioning:

- New accounts require written approval from management
- Access provisioned based on job role and responsibilities
- Default accounts disabled or removed
- Accounts activated only after background check completion

Account Reviews:

- Quarterly review of all active user accounts
- Annual comprehensive access rights review

- Removal of inactive accounts after 90 days
- Immediate deactivation of terminated employee accounts

Privileged Access:

- Administrative access strictly controlled and monitored
- Privileged accounts use separate credentials from standard accounts
- All privileged access logged and reviewed
- Emergency access procedures documented

4.4 Remote Access

- All remote access via secure VPN or encrypted connections
- Multi-factor authentication required
- Remote access sessions time out after 30 minutes of inactivity
- Remote access logs monitored for suspicious activity

---

5. DATA SECURITY

5.1 Encryption Standards

Data in Transit:

- All data transmitted over networks encrypted using TLS 1.2 or higher
- Internal network traffic on trusted networks may use lower encryption
- No unencrypted transmission of L3 sensitive data

Data at Rest:

- All L3 sensitive data encrypted using AES 256 or stronger
- Encryption keys managed securely with access controls
- Platform-level encryption provided by Salesforce and AWS

5.2 Data Storage

Approved Storage Locations:

- Salesforce (CRM and customer data)
- Amazon Web Services (cloud infrastructure and file storage)
- Company-issued devices with full-disk encryption

Prohibited Storage:

- Personal email accounts
- Personal cloud storage (Dropbox, Google Drive personal accounts, etc.)
- Unencrypted removable media
- Unsecured file sharing services

5.3 Data Transmission

- Customer data transmitted only via secure, encrypted channels
- Email attachments containing L3 data must be password-protected or encrypted
- Large file transfers use secure file transfer protocols
- No customer data transmitted via SMS or unencrypted messaging

5.4 Data Retention and Disposal

Retention Periods:

- Customer audio/video: Per customer instructions (default 2 weeks for post-production)
- Live captioning audio: Deleted immediately after delivery
- Customer account data: Duration of business relationship + legal requirements

- Financial records: 7 years per IRS requirements
- Security logs: Minimum 12 months

Secure Disposal:

- Electronic media sanitized using industry-standard wiping tools
- Physical media destroyed through shredding or incineration
- Certificates of destruction maintained for sensitive disposals
- Hard drives physically destroyed before disposal

---

6. NETWORK SECURITY

6.1 Network Architecture

- Logical network segmentation between production and non-production environments
- Firewalls protect network perimeter and critical systems
- Intrusion detection and prevention systems monitor network traffic
- Regular vulnerability scanning of network infrastructure

6.2 Wireless Security

- Wireless networks use WPA3 or WPA2 encryption minimum
- Guest wireless networks segregated from corporate network
- Wireless access points regularly updated with security patches
- Unauthorized wireless access points prohibited

6.3 Network Monitoring

- 24/7 monitoring by IT security partner
- Automated alerts for suspicious network activity
- Regular review of network logs
- Network traffic analysis for anomalies

---

7. ENDPOINT SECURITY

7.1 Device Management

Company-Issued Devices:

- Full-disk encryption required on all laptops and mobile devices
- Antivirus/anti-malware software installed and updated
- Automatic security updates enabled
- Remote wipe capability for lost or stolen devices

Personal Devices (BYOD):

- Not permitted to access or store L3 customer data
- If used for business email, must comply with security requirements
- MFA required for any business system access
- Subject to remote wipe if business data stored

7.2 Software and Patch Management

- Operating systems and applications kept up to date
- Critical security patches applied within 30 days of release
- High-priority patches applied within 15 days
- Software updates tested before production deployment
- End-of-life software replaced or upgraded

7.3 Antivirus and Anti-Malware

- Antivirus software installed on all endpoints
- Daily signature updates
- Real-time scanning enabled
- Weekly full system scans
- Quarantine and remediation procedures for detected threats

---

8. PHYSICAL SECURITY

8.1 Facility Access

- Office access restricted to authorized personnel
- Visitor sign-in and escort procedures
- After-hours access logged and monitored
- Keys and access cards controlled and tracked

8.2 Workstation Security

- Screens locked when unattended (auto-lock after 10 minutes)
- Clean desk policy for sensitive documents
- Secure storage for physical media containing sensitive data
- Visitor areas separated from work areas containing sensitive information

8.3 Equipment Security

- Company equipment inventoried and tracked
- Laptops secured with cable locks when in public spaces
- Portable media encrypted and password-protected
- Equipment disposal follows secure procedures

---

9. CLOUD AND THIRD-PARTY SECURITY

9.1 Cloud Service Providers

Aberdeen relies on the following primary cloud platforms:

Salesforce:

- SOC 2 Type II certified
- ISO 27001 certified
- GDPR compliant
- Regular security audits and penetration testing

Amazon Web Services (AWS):

- SOC 2 Type II certified
- ISO 27001 certified
- GDPR compliant
- Extensive security controls and certifications

9.2 AI Service Providers

When customers select AI-powered transcription:

- AWS Transcribe, Deepgram, Speechmatics, OpenAI Whisper
- Zero-retention policies where available
- Contractual prohibition on using customer data for AI training
- Data processing agreements in place
- Security and privacy commitments documented

9.3 Third-Party Risk Management

Vendor Assessment:

- Security assessment before engaging vendors with data access
- Review of vendor security certifications and policies
- Data processing agreements required for vendors processing customer data
- Annual vendor security reviews

Vendor Requirements:

- Appropriate security controls for data protection
- Compliance with applicable regulations
- Incident notification obligations
- Right to audit vendor security controls

---

10. SECURITY AWARENESS AND TRAINING

10.1 Training Requirements

All Personnel:

- Security awareness training upon hire
- Monthly security and privacy training sessions
- Annual comprehensive security training
- Specialized training based on role and data access
- Training completion tracked and documented

Training Topics:

- Information security policies and procedures
- Data classification and handling
- Password security and authentication
- Phishing and social engineering awareness
- Incident reporting procedures
- Privacy and data protection requirements
- Secure remote work practices

10.2 Security Communications

- Regular security updates and reminders
- Security bulletins for emerging threats
- Security tips and best practices
- Incident lessons learned shared (when appropriate)

10.3 Confidentiality Agreements

- All employees and contractors sign confidentiality agreements (NDAs)
- Non-compete agreements required where applicable
- Agreements reviewed and re-signed annually
- Obligations survive employment termination

---

11. INCIDENT RESPONSE AND MANAGEMENT

11.1 Incident Definition

A security incident includes:

- Unauthorized access to systems or data
- Data breaches or data loss

- Malware infections
- Denial of service attacks
- Physical security breaches
- Lost or stolen devices containing sensitive data
- Any suspected compromise of information assets

11.2 Incident Reporting

Immediate Reporting Required:

- All suspected security incidents must be reported immediately
- Report to: matt@aberdeen.io and deepthi@aberdeen.io
- IT security partner notified for immediate response
- Do not attempt to investigate or remediate alone

Reporting Channels:

- Email to security contacts
- Phone to President or Executive Vice President
- Direct contact with IT security partner

11.3 Incident Response Process

1. Detection and Reporting

- Incident identified through monitoring or user report
- Initial assessment of incident scope and severity

2. Containment

- Immediate actions to limit incident spread
- Affected systems isolated or taken offline if necessary
- Evidence preserved for investigation

3. Investigation

- Root cause analysis
- Determination of affected data and systems
- Documentation of incident timeline and actions

4. Notification

- Customer notification within 72 hours if customer data affected
- Regulatory notification as required by law
- Internal stakeholder communication

5. Remediation

- Security vulnerabilities addressed
- Affected systems restored or rebuilt
- Enhanced controls implemented

6. Post-Incident Review

- Lessons learned documented
- Policies and procedures updated
- Additional training provided if needed

11.4 Business Continuity

- Incident response procedures tested annually
- Business continuity plan maintained and updated
- Critical systems and data backed up regularly
- Disaster recovery plan tested annually

12. LOGGING AND MONITORING

12.1 Security Logging

Systems Requiring Logging:

- All systems processing customer data
- Authentication systems and access controls
- Firewalls and network security devices
- Critical business applications
- Administrative access to all systems

Log Contents:

- User identification
- Date and time of activity
- Type of activity or event
- Success or failure of activity
- Source and destination of activity

12.2 Log Management

- Logs retained for minimum 12 months
- Logs protected from unauthorized modification
- Log review procedures for detecting anomalies
- Automated alerting for critical security events
- Centralized log management where possible

12.3 Monitoring and Alerting

- 24/7 security monitoring by IT security partner
- Automated alerts for:
    - Failed login attempts
    - Privilege escalation
    - Unusual data access patterns
    - System configuration changes
    - Malware detection
    - Network intrusion attempts

13. SECURE DEVELOPMENT AND CHANGE MANAGEMENT

13.1 Configuration Management

While Aberdeen primarily uses commercial platforms (Salesforce, AWS):

- Configuration changes documented and approved
- Change management process for system modifications
- Testing of changes in non-production environment
- Rollback procedures for failed changes
- Configuration baselines maintained

13.2 API and Integration Security

- Secure API authentication required
- API keys and credentials protected
- API rate limiting and monitoring
- Regular security review of integrations

- Third-party integrations assessed for security

---

14. BUSINESS CONTINUITY AND DISASTER RECOVERY

14.1 Business Continuity Planning

- Business continuity plan documented and maintained
- Critical business functions identified
- Recovery time objectives (RTO): 12-24 hours
- Recovery point objectives (RPO): 4-8 hours
- Plan tested annually

14.2 Data Backup

- Regular backups of critical data and systems
- Systems backed up across multiple AWS Availability Zones per AWS and Salesforce recommendations
- Backup integrity verified regularly
- Backups stored in geographically separate locations for redundancy
- Backup restoration tested quarterly
- Backup retention per data retention policies

14.3 Disaster Recovery

- Disaster recovery procedures documented
- Leverages Salesforce and AWS platform redundancy
- Communication plan for major incidents
- Alternative work arrangements documented
- Annual disaster recovery testing

---

15. COMPLIANCE AND LEGAL REQUIREMENTS

15.1 Regulatory Compliance

Aberdeen maintains compliance with:

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA/CPRA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA) when applicable
- Other applicable state and federal privacy laws

15.2 Contractual Obligations

- Data Processing Agreements with customers
- Service Level Agreements (SLAs)
- Non-Disclosure Agreements (NDAs)
- Vendor contracts and agreements
- Terms of Service and Privacy Policy

15.3 Audits and Assessments

Internal Reviews:

- Quarterly security control reviews
- Annual comprehensive policy review
- Regular access rights reviews
- Periodic security self-assessments

External Assessments:

- Customer security questionnaires and assessments
- Third-party security audits when required
- Penetration testing (planned for implementation)
- Compliance certifications (planned: SOC 2, ISO 27001)

---

16. PRIVACY AND DATA PROTECTION

16.1 Privacy Principles

Aberdeen adheres to the following privacy principles:

- Data minimization - collect only necessary information
- Purpose limitation - use data only for specified purposes
- Transparency - clear communication about data practices
- Data subject rights - facilitate exercise of individual rights
- Accountability - demonstrate compliance with obligations

16.2 Customer Data Protection

Processing Commitments:

- Process customer data only per customer instructions
- Implement appropriate security measures
- Assist with data subject rights requests
- Notify of security incidents within 72 hours
- Return or delete data upon request
- Never use customer data for AI model training

16.3 Employee Privacy

- Employee personal information protected
- Access to employee data restricted
- Employee privacy rights respected
- Data retention per employment records requirements

---

17. ACCEPTABLE USE

17.1 Acceptable Use of Systems

Aberdeen systems and resources may be used only for:

- Legitimate business purposes
- Authorized activities within job responsibilities
- Compliance with all policies and legal requirements

17.2 Prohibited Activities

The following activities are strictly prohibited:

- Unauthorized access to systems or data
- Sharing credentials or access rights
- Installing unauthorized software
- Bypassing security controls
- Using systems for illegal activities
- Harassment or inappropriate communications
- Personal use that interferes with business operations
- Storing or transmitting offensive or inappropriate material

- Attempting to compromise security

17.3 Internet and Email Use

- Internet use primarily for business purposes
- Limited personal use permitted if not interfering with work
- No downloading or streaming of illegal content
- Email communications professional and appropriate
- Caution with email attachments and links (phishing awareness)
- Company email subject to monitoring

---

18. MOBILE DEVICE AND REMOTE WORK

18.1 Mobile Device Security

Company-Issued Devices:

- Full-disk encryption required
- Strong passcode/biometric authentication
- Automatic screen lock (10 minutes)
- Remote wipe capability enabled
- Lost or stolen devices reported immediately

Personal Devices (BYOD):

- Not permitted for processing or storing customer data
- If used for business email, must meet security requirements
- MFA required for system access
- Subject to remote wipe of business data
- Personal liability for device security

18.2 Remote Work Security

- Secure home network with WPA2/WPA3 encryption
- VPN required for remote access to internal systems
- Physical security of workspace (privacy from family members)
- Screen privacy when working in public spaces
- Secure disposal of printed materials
- Video conferencing security best practices

---

19. HUMAN RESOURCES SECURITY

19.1 Pre-Employment

- Background checks for all employees with data access
- Reference checks
- Verification of education and credentials
- Security roles and responsibilities communicated

19.2 During Employment

- Annual security training
- Monthly security awareness sessions
- Performance reviews include security compliance
- Job changes trigger access review and adjustment
- Disciplinary procedures for security violations

19.3 Termination

Immediate Actions Upon Termination:

- All access rights revoked immediately
- Company equipment returned
- Exit interview covering security obligations
- Reminder of ongoing confidentiality obligations
- Final paycheck withheld until equipment returned

Offboarding Checklist:

- Systems access revoked
- Email account disabled or forwarded
- Physical access cards deactivated
- Keys returned
- Company devices wiped and reimaged
- Customer data deleted from personal devices

---

20. POLICY ENFORCEMENT

20.1 Compliance Monitoring

- Regular compliance audits and reviews
- Automated monitoring where possible
- Security incident tracking and analysis
- Policy violation investigation and documentation

20.2 Violations and Consequences

Violations of this policy may result in:

- Verbal or written warning
- Mandatory retraining
- Suspension of system access
- Disciplinary action up to and including termination
- Legal action if warranted
- Referral to law enforcement for criminal activity

20.3 Reporting Violations

- Security policy violations must be reported
- No retaliation for good faith reporting
- Anonymous reporting available if needed
- Investigation of all reported violations

---

21. POLICY MAINTENANCE

21.1 Policy Review and Updates

- Annual comprehensive review of all security policies
- Updates as needed for regulatory changes
- Updates based on incidents or lessons learned
- Technology changes trigger policy review
- Employee feedback incorporated when appropriate

21.2 Policy Approval

- Policy changes approved by President and Executive Vice President
- Major changes communicated to all personnel

- All personnel acknowledge receipt and understanding
- Policy version control maintained

21.3 Related Policies

This policy is supported by the following related policies and procedures:

- Privacy Policy
- Data Processing Agreement
- Incident Management and Data Breach Response Policy
- Access Control and Authentication Policy
- Change Management and Patch Management Policy
- Log Management and Monitoring Policy
- Vendor and Third-Party Risk Management Policy
- Asset Management Policy
- Business Continuity and Disaster Recovery Plan
- Risk Management Policy

---

22. EXCEPTIONS

22.1 Exception Process

- Requests for policy exceptions submitted in writing
- Business justification required
- Risk assessment performed
- Compensating controls identified
- Approval by President or Executive Vice President required
- Exceptions documented and reviewed regularly
- Temporary exceptions include expiration date

22.2 Exception Review

- All exceptions reviewed quarterly
- Reauthorization required annually
- Exceptions revoked when no longer needed
- Exception log maintained

---

23. CONTACT INFORMATION

23.1 Security Contacts

For Security Incidents or Questions:

President: Matthew Cook
Email: matt@aberdeen.io
Phone: +1(949)216-1056
Executive Vice President: Deepthi Yathiender
Email: deepthi@aberdeen.io
Phone: +1(949)858-4463

23.2 General Information

Aberdeen Captioning Inc.
DBA: Aberdeen Broadcast Services
30211 Avenida de las Banderas, Suite 110
Rancho Santa Margarita, CA 92688

24. POLICY ACKNOWLEDGMENT

All employees and contractors must acknowledge that they have:

- Received and read this Information Security Policy
- Understand the requirements and their responsibilities
- Agree to comply with all policy provisions
- Understand that violations may result in disciplinary action

30211 Avenida de las Banderas, Suite 110
Rancho Santa Margarita, CA 92688
[phone] 949.858.4463
aberdeen.io