AXIOM INC. · INFORMATION SECURITY POLICY

1. PURPOSE

This policy establishes security requirements for all Axiom employees, contractors, and third parties who access Axiom systems and data.

2. CLASSIFICATION OF DATA

Public: Marketing materials, blog posts, open-source code.
Internal: Slack messages, internal docs, meeting notes.
Confidential: Customer data, financials, employee PII, source code.
Restricted: Encryption keys, access credentials, security audit reports.

3. ACCESS CONTROL

All systems require multi-factor authentication (MFA).
Access follows the principle of least privilege.
Manager approval required for production system access.
Quarterly access reviews conducted by the Security team.
Immediate access revocation upon employee separation.

4. DEVICE SECURITY

Company devices must have full-disk encryption enabled.
Screen lock required after 5 minutes of inactivity.
Personal devices may access email only via the approved MDM solution.
No company data on personal USB drives or cloud storage accounts.

5. INCIDENT RESPONSE

If you suspect a security incident:
a) Do NOT attempt to fix it yourself.
b) Report immediately to security@axiom.io or the Slack channel.
c) Preserve evidence such as screenshots and logs.
d) The Security team will respond within 1 hour during business hours.

6. ACCEPTABLE USE

Company systems are for business use; limited personal use is acceptable.
No torrenting, illegal downloads, or unapproved software installation.
VPN required when connecting from public networks.
Annual security awareness training is mandatory (due by March 31 each year).

7. COMPLIANCE

Axiom complies with SOC 2 Type II, GDPR, and CCPA requirements.
All employees handling customer data must complete privacy training annually.