## 1. IT Security Policy

**Objective**: Ensure confidentiality, integrity, and availability of data, systems, and AI-based products.

### 1.1 Data Protection

- **Encryption**: All data (at rest and in transit) encrypted using AES-256 and TLS 1.3.
- **AI Model Security**: Rigorous testing for adversarial attacks, model inversion, and data poisoning.
- **Access Control**: Role-based access (RBAC) with multi-factor authentication (MFA) for sensitive systems.

### 1.2 Incident Response

- **Procedure**: Immediate isolation, forensic analysis, and stakeholder notification within 2 hours of breach detection.
- **AI-Specific Threats**: Continuous monitoring for model drift and unauthorized API access.

### 1.3 Compliance

- Adherence to GDPR, ISO 27001, NIST AI Risk Management Framework, and CCPA.
- Regular third-party penetration testing and SOC 2 audits.

---

## 2. IT Management Framework

**Objective**: Streamline development, deployment, and maintenance of AI products.

### 2.1 Infrastructure

- **Cloud Services**: AWS/GCP/Azure with Kubernetes for scalable AI workloads.
- **Monitoring**: Real-time dashboards (e.g., Grafana) for system health, API latency, and model performance.

### 2.2 Software Development Lifecycle (SDLC)

- **Phases**:
    1. **Planning**: Risk assessment for AI ethics and bias.
    2. **Development**: CI/CD pipelines with automated testing (unit, integration, bias detection).

3. **Deployment**: Canary releases with rollback protocols.

**2.3 Maintenance**

- **Patch Management**: Monthly updates for OS, libraries, and AI frameworks (TensorFlow, PyTorch).
- **Disaster Recovery**: Geo-redundant backups and 99.9% uptime SLA.

---

**3. HR Management Policies**

**Objective**: Foster a skilled, ethical, and security-conscious workforce.

**3.1 Recruitment & Training**

- **Hiring**: Background checks for roles handling sensitive data or AI models.
- **Training**:
  - Annual workshops on AI ethics, GDPR, and cybersecurity.
  - Certifications (e.g., AWS Certified ML Specialist, CISSP).

**3.2 Employee Conduct**

- **Code of Ethics**: Prohibition of unauthorized data use or biased AI model development.
- **Confidentiality**: NDAs for all employees and contractors.

**3.3 Performance Management**

- **KPIs**: Alignment with project milestones (e.g., model accuracy, compliance deadlines).
- **Whistleblower Policy**: Anonymous reporting channels for ethical concerns.

---

**4. Other Management Policies**

**4.1 Risk Management**

- **AI Risk Assessment**: Bias audits, explainability reports, and environmental impact analysis.
- **Vendor Management**: Third-party vendors must comply with ISO 27001 and GDPR.

**4.2 Compliance & Governance**

- **AI Governance Board**: Oversees ethical AI use, chaired by CTO and legal counsel.
- **Documentation**: Maintained for audit trails, model versions, and data lineage.

**4.3 Customer Assurance**

- **SLAs**: 24/7 technical support, incident resolution within 6 hours.
- **Transparency**: Provide model explainability reports and data usage policies to clients.

---

**5. Conclusion**

This document validates [Company Name]'s commitment to delivering secure, ethical, and high-quality AI solutions. Our policies align with global standards and ensure resilience against evolving threats.

**Appendices**:

- References: ISO 27001, NIST AI RMF, GDPR.
- Contact: [Security Team Email, Compliance Officer Phone].