BLINKSIGNS

AI Governance Checklist for Autonomous Digital Signage

This checklist provides an enterprise control framework for predictive and agentic AI systems running digital signage networks. Customize it to your regulatory, operational, and risk requirements.

Pre-Deployment Readiness

Access Control & Permissions

- [ ] Role-based access control (RBAC) implemented with least-privilege model
- [ ] Content creator, approver, admin, and AI operator roles defined
- [ ] Multi-factor authentication enabled for all administrative accounts
- [ ] Regular access reviews scheduled (quarterly minimum)
- [ ] Offboarding process includes immediate AI system access revocation

Content Approval Workflows

- [ ] AI-generated content requires human approval before first publish
- [ ] Tiered approval process defined for high-risk verticals (pharma, finance, healthcare)
- [ ] Brand safety guidelines programmed into AI guardrails
- [ ] Legal/compliance review process for regulated messaging
- [ ] Emergency override capability for inappropriate content

Audit & Accountability

- [ ] Full audit trail logging enabled for all AI decisions
- [ ] Timestamp, model version, input data, and output content captured
- [ ] Content provenance tracking (who created, who approved, what AI generated)
- [ ] Log retention policy aligned with regulatory requirements (typically 2–7 years)
- [ ] Audit reports accessible to compliance and security teams

877.433.4466 sales@blinksigns.com www.blinksigns.com

BLINKSIGNS

Operational Controls

Model Management

- [ ] Model version control system in place
- [ ] Track which AI model version is deployed to which screen/location
- [ ] Rollback capability tested and documented
- [ ] A/B testing framework for new model versions before full rollout
- [ ] Performance benchmarks defined for model acceptance

Monitoring & Alerts

- [ ] Anomaly detection configured for unexpected content changes
- [ ] Performance drop alerts trigger human review
- [ ] Policy violation notifications sent to governance team
- [ ] Override rate monitored (should decrease over time)
- [ ] Model confidence trends tracked and reviewed monthly

Privacy & Data Protection

- [ ] Privacy Impact Assessment (PIA) completed and documented
- [ ] Data collection inventory maintained (what, why, how long)
- [ ] GDPR/CCPA/regional compliance verified
- [ ] Anonymous analytics confirmed (no PII collection)
- [ ] Data retention and deletion policies enforced

Incident Response

Kill-Switch & Rollback

- [ ] Emergency content revert procedure documented
- [ ] Kill-switch tested quarterly
- [ ] Backup “safe” content library maintained
- [ ] Incident escalation path defined (who to contact, when)
- [ ] Post-incident review process established

877.433.4466
sales@blinksigns.com
www.blinksigns.com

BLINKSIGNS

Continuous Improvement

- [ ] Quarterly governance review meetings scheduled
- [ ] Stakeholder feedback loop established (marketing, IT, legal, ops)
- [ ] Governance documentation updated as system evolves
- [ ] Training programs for new team members on AI controls
- [ ] External audit capability (third-party review if needed)

Multi-Location & Regional Considerations

Consistency Across Networks

- [ ] Governance controls enforced uniformly across all regions
- [ ] Local regulatory requirements mapped and addressed
- [ ] Regional content approval workflows accommodate local languages/cultures
- [ ] Centralized oversight with local autonomy balanced

Vendor & Integration Governance

- [ ] AI vendor contracts include data usage and ownership clauses
- [ ] Third-party integrations (POS, CRM, ERP) reviewed for security
- [ ] API authentication and authorization standards enforced
- [ ] Vendor SLAs aligned with business continuity requirements

Sign-Off & Approval

Role	Name	Signature	Date
Chief Marketing Officer			
Chief Information Officer			
Chief Privacy Officer / DPO			
Legal / Compliance Lead			

Next Review Date:

Document Owner:

Contact for Questions:

877.433.4466 sales@blinksigns.com www.blinksigns.com