Surface3D AI Governance Framework

Document Version: 1.0
Effective Date: March 31, 2026
Last Reviewed: March 31, 2026
Owner: Surface3D Engineering & Compliance

---

1. Purpose

This document establishes Surface3D's governance framework for the use of artificial intelligence (AI) and machine learning (ML) technologies within our platform. It defines policies, procedures, and controls governing the responsible development, deployment, and operation of AI capabilities to ensure ethical use, data protection, regulatory compliance, and alignment with customer expectations.

---

2. Scope

This framework applies to all AI and ML services integrated into the Surface3D platform, including:

- **Text-to-Image Generation**: Google Gemini, Google Imagen, OpenAI DALL-E 3, Flux (via Replicate), and Recraft v3
- **Image Analysis**: GPT-4o-mini vision analysis for prompt refinement
- **Background Removal**: Client-side ML-based background removal (@imgly/background-removal)
- **Image Upscaling**: AI-powered image enhancement

This framework covers all data processed by these AI services, all personnel involved in AI operations, and all customer data that interacts with AI features.

---

3. AI Data Usage Policy (No-Training Policy)

3.1 Core Commitment

Surface3D does not use customer data to train, fine-tune, or improve any AI or machine learning models. This commitment is absolute and applies to all AI providers integrated into our platform.

3.2 Data Flow Architecture

Customer data interacts with AI services exclusively through **transient, stateless API calls**:

1. **Input**: User-provided text prompts, optional reference images (transmitted as data URLs only), and optional logos are sent to the selected AI provider's API.
2. **Processing**: The AI provider generates an image based on the input.
3. **Output**: The generated image is returned to Surface3D and stored in the customer's designated storage path.
4. **No Retention by AI Providers**: All API calls are made under terms that prohibit the AI provider from retaining, storing, or using customer inputs or outputs for model training.

3.3 Provider-Specific Data Handling

AI Provider	API Terms	Training Opt-Out	Data Retention by Provider
Google Gemini (Vertex AI)	Google Cloud Terms of Service	Opted out via API usage terms	No input/output retention for training
Google Imagen (Vertex AI)	Google Cloud Terms of Service	Opted out via API usage terms	No input/output retention for training
OpenAI (DALL-E 3)	OpenAI Business API Terms	API data not used for training per OpenAI API data usage policy	No input/output retention for training
Replicate (Flux, Recraft)	Replicate Terms of Service	API data not used for training per Replicate terms	No input/output retention for training
@imgly Background Removal	Client-side processing	N/A -- runs entirely in user's browser	No data leaves the client

3.4 Reference Image Protection

To prevent unintended data leakage, Surface3D enforces strict controls on reference images:

- Reference images are transmitted only as **base64-encoded data URLs** -- never as publicly accessible URLs
- This prevents AI providers from accessing customer design templates or proprietary artwork beyond the immediate API call
- Reference images are used solely for style guidance in the current generation request

3.5 Customer Logo Handling

Customer logos uploaded for AI-assisted design:

- Are transmitted to the AI provider only when explicitly included by the user in a generation request
- Are not stored by AI providers beyond the duration of the API call
- Remain under the customer's control in their designated Firebase Cloud Storage path

---

4. Data Deletion Policy

4.1 Customer Data Deletion Rights

Surface3D supports data deletion requests in compliance with applicable data protection regulations (GDPR, CCPA, and similar frameworks).

4.2 Scope of Deletable Data

Upon a verified data deletion request, Surface3D will delete:

- **User profile data** (Supabase `users` table)
- **Organization membership records** (Supabase `org_members` table)
- **Design projects and associated assets** (Supabase `projects`, `project_assets` tables)
- **Generated textures and uploaded images** (Firebase Cloud Storage: `textures/{userId}/`)
- **3D model files** (Firebase Cloud Storage: `models/{userId}/`)
- **Scene snapshots** (Firebase Cloud Storage: `snapshots/{userId}/`)
- **Editor state files** (Firebase Cloud Storage: `editorStates/{userId}/`)
- **Credit transaction history** (Supabase `credit_transactions` table)
- **Activity/audit logs** (Supabase `activities` table)
- **Authentication records** (Firebase Authentication)

4.3 Deletion Process

1. **Request**: Customer submits a data deletion request via email to the designated privacy contact.
2. **Verification**: Identity verification is performed to confirm the requestor's authorization.
3. **Acknowledgment**: Request is acknowledged within 48 hours.
4. **Execution**: All identifiable customer data is deleted from production systems within 30 calendar days.

5. **Backup Purge**: Data is purged from backups within the next backup rotation cycle (maximum 90 days).
6. **Confirmation**: Written confirmation of deletion is provided to the customer.

4.4 Data Retention Exceptions

The following data may be retained after a deletion request for legitimate business or legal purposes:

- Aggregated, anonymized usage analytics (no personally identifiable information)
- Financial transaction records required for tax and accounting compliance (retained per applicable law)
- Data required to be retained by law enforcement or regulatory order

4.5 Third-Party Data Deletion

Upon customer data deletion:

- **Stripe**: Payment records are retained by Stripe per their data retention policy and PCI-DSS requirements. Customers may separately request deletion from Stripe.
- **AI Providers**: No customer data is retained by AI providers (see Section 3.3), so no deletion action is required.
- **Firebase Authentication**: User authentication record is deleted.

---

5. AI Model Selection and Evaluation

5.1 Provider Evaluation Criteria

Before integrating any AI provider, Surface3D evaluates:

- **Data usage policies**: Provider must not use API inputs/outputs for model training
- **Security certifications**: SOC 2, ISO 27001, or equivalent
- **Data residency**: Compliance with applicable data residency requirements
- **API terms of service**: Must support enterprise/business-tier terms prohibiting data retention for training
- **Output quality and safety**: Must include content safety filters

5.2 Content Safety

All AI generation endpoints include:

- **Input validation**: Prompts are validated and sanitized before submission to AI providers
- **Output filtering**: AI providers' built-in content safety filters are enabled
- **Rate limiting**: 10 requests per minute per user to prevent abuse
- **Audit logging**: All generation requests are logged with user ID, model used, credit cost, and timestamp
- **Timeout protection**: 45-second timeout on generation requests, 15-second timeout on vision analysis

---

6. Transparency and Accountability

6.1 Customer Transparency

- Customers are informed that AI-generated designs are produced by third-party AI models
- The specific AI model used for each generation is logged and available in audit records
- Customers can select their preferred AI model from available options
- Credit costs are displayed before generation and itemized in transaction history

6.2 Internal Accountability

- AI governance policies are reviewed quarterly
- Changes to AI providers or data handling practices require documented review and approval
- All AI-related incidents (data exposure, model failures, policy violations) are logged and investigated
- Annual review of all AI provider agreements and data handling practices

---

7. Risk Management

7.1 Identified Risks and Mitigations

Risk	Likelihood	Impact	Mitigation
AI provider changes data usage policy	Low	High	Quarterly review of provider terms; contractual protections; ability to switch providers
Generated content contains inappropriate material	Low	Medium	Provider content safety filters; user reporting mechanism; audit logging
Customer data exposed through AI API calls	Very Low	High	Data URL-only transmission; no persistent storage at provider; encryption in transit
AI service outage	Medium	Medium	Multi-provider architecture with automatic fallback; graceful degradation
Excessive API costs from abuse	Low	Medium	Per-user rate limiting; credit-based access control; usage monitoring

7.2 Incident Response

AI-specific incidents (e.g., suspected data exposure, content safety failures) are handled under Surface3D's standard incident response process with the following additions:

- Immediate suspension of the affected AI provider integration
- Assessment of data exposure scope
- Customer notification within 72 hours if personal data was affected
- Remediation and root cause analysis within 14 days

---

8. Regulatory Compliance

Surface3D's AI governance framework is designed to comply with:

- **GDPR** (General Data Protection Regulation) -- EU data protection
- **CCPA/CPRA** (California Consumer Privacy Act / California Privacy Rights Act) -- California data protection
- **EU AI Act** -- AI-specific regulation (Surface3D's use of AI falls under limited/minimal risk categories as a creative tool)
- **SOC 2 Type II** -- alignment with trust service criteria for security, availability, and confidentiality

9. Review and Updates

This framework is reviewed and updated:

- **Quarterly**: Routine review of AI provider terms and emerging regulations
- **Upon Change**: When new AI providers are integrated, existing providers change their terms, or regulatory requirements change
- **Annually**: Comprehensive review including risk assessment update

10. Contact

For questions about this AI Governance Framework or to submit a data-related request:

Surface3D Privacy & Compliance

Email: support@surface3d.ai

This document is maintained by Surface3D Engineering & Compliance and is subject to periodic review and updates.