

AI-Supported Work Authorization

Gate Decision Record

Use this record to connect evidence to an explicit decision at Stages 0–5. Completing reviews, tests, or training does not itself authorize the work.

Use ID	Unique identifier linked to the AI Use Inventory
Decision record ID / version	
Stage	☐ 0 Inventory ☐ 1 Define risk ☐ 2 Authority/records ☐ 3 Test ☐ 4 Routine use ☐ 5 Change/retire
Decision requested	Register, contain, prohibit, authorize pilot, authorize routine use, expand, narrow, reinstate, suspend, stop, or retire
Decision date / effective date	
Next review date or trigger	

Handling note

Do not enter passwords, API keys, access tokens, full personal data, protected record content, or confidential prompts. Cite controlled repositories and evidence identifiers. Store this record under the applicable access, retention, and signature controls.

1. Bounded use and decision context

AI-supported task	Describe the specific work, not a general platform or vendor
Expected output and downstream decision	State what the output supports and who decides
Named process, product, site, and jurisdiction	State what is inside and outside scope
System, model, version, interface, and configuration	Record the qualified state and evidence reference

Source boundary	Systems, repositories, document status, inclusion rules, exclusions, and unavailable sources
Users and assigned roles	Identify operators, reviewers, approvers, administrators, and support roles
Authority envelope	What the system may read, draft, recommend, change, execute, or approve
Prohibited actions and technical enforcement	Describe permissions, identity, approval checks, and stop controls
Failure consequences	Product quality, patient safety, data integrity, compliance, privacy, security, or availability
Records and signatures	Predicate-rule basis, Part 11 determination, required evidence, retention, and electronic-signature use

2. Accountability

Role	Name / function	Responsibility for this decision	Conflict / independence note
Process owner			
Quality owner / quality unit			
System owner			
Data owner			
Evaluation owner			
IT / security / privacy			
Supplier / external party			

3. Evidence reviewed

Evidence / control	Status / reviewer	Reference
☐ Current AI Use Inventory entry and ownership		
☐ Intended use, baseline process, risk assessment, and applicable requirements		
☐ Data map, source inventory, inclusion rules, and evidence identity		
☐ Authority design, access controls, prohibited actions, and segregation of duties		
☐ Part 11 / electronic-record and signature determination where applicable		
☐ Security, privacy, and third-party dependency review		
☐ Supplier evidence and change-notification responsibilities		
☐ Representative challenge cases, scoring rubric, and protected holdout evidence		
☐ Human reviewer qualification and assessor calibration		
☐ Recovery, duplicate request, interrupted execution, and partial-success tests		
☐ Pilot results, critical failures, near misses, overrides, workload, and user feedback		
☐ Benefit and burden: time to acceptable work, correction, escalation, maintenance, and rework		
☐ Change impact, regression evidence, requalification, continuity, and retirement plan		

4. Security, privacy, and data-integrity disposition

Authentication and identity	Identify the user/system identity and whether a handle, URL, shared credential, or weak bearer identifier creates exposure
Access and least privilege	Show that technical permissions match the authority envelope; instructions alone are insufficient

Data classification and privacy	State personal, confidential, GxP, or cross-border data; identify minimization and approved storage
Third-party and script dependencies	List suppliers, integrations, embedded services, external scripts, and change/incident responsibilities
Decision provenance and audit evidence	Inputs, versions, retrievals, output, changes, human reasons, approvals, and resulting state
Retention and uncontrolled copies	Keep enough evidence to explain the decision without indiscriminate logging
Incident, stop, and recovery controls	Detection, containment, reconciliation, compensating action, notification, and suspension authority
Security / privacy disposition	☐ Acceptable ☐ Acceptable with actions ☐ Not acceptable ☐ Not applicable; cite reviewer and evidence

5. Evaluation findings and uncertainty

Evaluation design	Conditions compared, sample, case classes, versions, reviewer instructions, blinding, and holdout protection
Predefined thresholds and critical failures	Cite the approved scoring sheet and decision rules
Results	Completed cases, average score, critical failures, disagreements, withdrawals, and time to acceptable output
Important failure modes	Consequential omissions, unsupported conclusions, rejected correct work, unnecessary escalation, and recovery failures
Reviewer performance and workload	Competence, evidence access, review time, queue, escalation patterns, and practical authority

Benefit and cost	Compare the complete job with the baseline, including control and maintenance burden
Limitations and unresolved uncertainty	State what was not tested, small-sample uncertainty, unavailable evidence, or supplier constraints
Corrective actions required before decision	Owner, due date, evidence needed, and whether use remains restricted

6. Gate decision

Select one decision. The written scope and conditions govern; the checkbox alone is not authorization.

☐ Register / assign ownership
 ☐ Contain or prohibit
 ☐ Authorize bounded pilot
 ☐ Correct and retest
☐ Authorize routine use
 ☐ Authorize expansion
 ☐ Narrow or restrict
 ☐ Suspend / stop
 ☐ Reinstate
 ☐ Retire

Decision rationale	Explain how the evidence supports the decision and identify contrary evidence
Authorized scope	Task, sources, system/version, users, site/product, authority, operating hours, and output destination
Conditions and open actions	Owner, due date, evidence required, and consequence of non-completion
Monitoring	Consequential performance, drift indicators, incidents, near misses, overrides, workload, and user feedback
Stop or restriction criteria	State the finding, threshold, incident, or unavailable control that triggers action
Change and re-review triggers	Model/version, retrieval, interface, procedure, product/site, staff, permission, supplier, or regulation

Effective period / expiry

State when the decision must be reconsidered even if no trigger occurs

7. Accountable approvals

Use the organization's approved approval and electronic-signature system where required. This Word template is not itself configured or validated as a Part 11 system.

Role	Name / title	Decision / signature reference	Date
Process owner			
Quality owner / quality unit			
System owner (as applicable)			
Data owner / privacy / security (as applicable)			

8. Attachments and revision history

Attachments / evidence index

List controlled identifiers and locations; do not embed protected source records here

Superseded decision records

Version	Date	Change / reason	Approved by

Template basis: Brian Drapeau, Governing AI in Pharmaceutical Operations, version 1.0 (2026), AI-Supported Work Authorization Cycle. Security prompts reflect the supplied September 18, 2026 review of gxpframe.com and lifesciencesai.academy; users must perform a current, use-specific assessment.