Collaboration AI Policy Discussion

CLAS Collaboration Meeting

November 17, 2026

Introduction

- JLab's Guidance on Using Generative SI Tools
  - https://jlab.servicenowservices.com/sp?s...5c1e0d6a47cda610281bbd51026d4340&id=kb_article_view&sysparm_rank=1&sysparm_tsqueryId=29f738323b889f10099d8c0864e45ab2
- CERN's General Principles for the Use of AI
  - https://home.cern/general-principles-use-ai-cern/
- APS's Appropriate Use of AI Tools
  - https://journals.aps.org/authors/appropriate-use-ai-tools
- FAIR Principles
  - Findable, Accessible, Interoperable, Reusable (and reproducible)
  - https://www.gofair.foundation/fair-principles

The collaboration's software working group has SI "best practices" (and general ones too)

- https://pages.jlab.org/hallb/clas12/swwg/ai-best-practices.html
- https://pages.jlab.org/hallb/clas12/swwg/best-practices.html

Recent Observations not in the US news

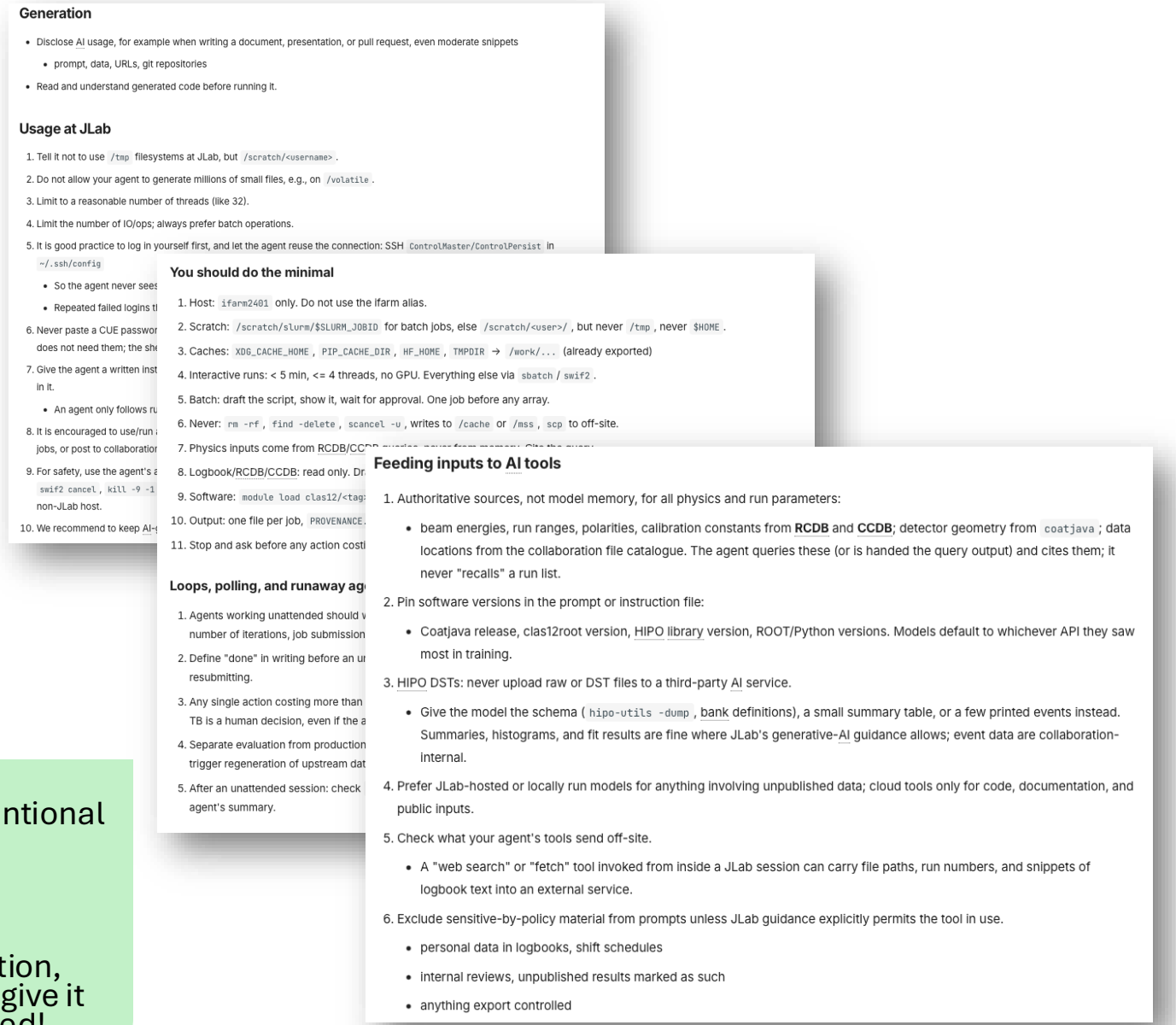
- Increase in `/volatile/clas12` write volume (1/lifetime) and file count (O(10^6))
- Antiquated filesystem usage, e.g., `/group/clas12`
- Simulations combining clas12 software spanning 10 years (!?)
- Overloading by SI agents of many JLab webservers, e.g. `clasweb`
- Overloading by (internal!) SI agents of JLab's GitLab server, `code.jlab.org`
- Missing AI/SI attribution, provenance, in software and analysis notes

The collaboration should consider official guidelines or rules regarding SI tools and their usage (!?)

1. Attribution in publications
   - Adopt APS Journals' policy, more?
2. Internal attribution and provenance
   - technical documentation, analysis notes, software
   - CERN's are general, more? includes user responsibilities
3. CLAS12 data access
   - The collaboration already has a policy regarding non-member data access

SWWG AI Best Practices

- Generated by SI based on the experience and instructions of Bhawani and others, plus manual edits
- Covers common pitfalls, some specific to JLab, most extrapolatable to anywhere, many come back to FAIR principles
- Needs cultivating and pruning, and will always be a living document of evolving best practices
  - *with lots of details not intended to be appropriate for collaboration "policy"*



Generation

- Disclose AI usage, for example when writing a document, presentation, or pull request, even moderate snippets
  - prompt, data, URLs, git repositories
- Read and understand generated code before running it.

Usage at JLab

1. Tell it not to use `/tmp` filesystems at JLab, but `/scratch/<username>`.
2. Do not allow your agent to generate millions of small files, e.g., on `/volatile`.
3. Limit to a reasonable number of threads (like 32).
4. Limit the number of IO/ops; always prefer batch operations.
5. It is good practice to log in yourself first, and let the agent reuse the connection: SSH `ControlMaster/ControlPersist` in `~/.ssh/config`
   - So the agent never sees
   - Repeated failed logins t
6. Never paste a CUE passwor
   does not need them; the she
7. Give the agent a written inst
   in it.
   - An agent only follows ru
8. It is encouraged to use/run a
   jobs, or post to collaboratior
9. For safety, use the agent's a
   `swif2 cancel`, `kill -9 -1`
   non-JLab host.
10. We recommend to keep AI-g

You should do the minimal

1. Host: `ifarm2401` only. Do not use the ifarm alias.
2. Scratch: `/scratch/slurm/$SLURM_JOBID` for batch jobs, else `/scratch/<user>/`, but never `/tmp`, never `$HOME`.
3. Caches: `XDG_CACHE_HOME`, `PIP_CACHE_DIR`, `HF_HOME`, `TMPDIR` → `/work/...` (already exported)
4. Interactive runs: < 5 min, <= 4 threads, no GPU. Everything else via `sbatch` / `swif2`.
5. Batch: draft the script, show it, wait for approval. One job before any array.
6. Never: `rm -rf`, `find -delete`, `scancel -u`, writes to `/cache` or `/mss`, `scp` to off-site.
7. Physics inputs come from RCDB/CCDB
8. Logbook/RCDB/CCDB: read only. Dr
9. Software: `module load clas12/<tag>`
10. Output: one file per job, `PROVENANCE`
11. Stop and ask before any action costl

Loops, polling, and runaway ag

1. Agents working unattended should v
   number of iterations, job submission
2. Define "done" in writing before an u
   resubmitting.
3. Any single action costing more than
   TB is a human decision, even if the a
4. Separate evaluation from production
   trigger regeneration of upstream dat
5. After an unattended session: check
   agent's summary.

Feeding inputs to AI tools

1. Authoritative sources, not model memory, for all physics and run parameters:
   - beam energies, run ranges, polarities, calibration constants from **RCDB** and **CCDB**; detector geometry from `coatjava`; data locations from the collaboration file catalogue. The agent queries these (or is handed the query output) and cites them; it never "recalls" a run list.
2. Pin software versions in the prompt or instruction file:
   - Coatjava release, clas12root version, HIPO library version, ROOT/Python versions. Models default to whichever API they saw most in training.
3. HIPO DSTs: never upload raw or DST files to a third-party AI service.
   - Give the model the schema (`hipo-utils -dump`, bank definitions), a small summary table, or a few printed events instead. Summaries, histograms, and fit results are fine where JLab's generative-AI guidance allows; event data are collaboration-internal.
4. Prefer JLab-hosted or locally run models for anything involving unpublished data; cloud tools only for code, documentation, and public inputs.
5. Check what your agent's tools send off-site.
   - A "web search" or "fetch" tool invoked from inside a JLab session can carry file paths, run numbers, and snippets of logbook text into an external service.
6. Exclude sensitive-by-policy material from prompts unless JLab guidance explicitly permits the tool in use.
   - personal data in logbooks, shift schedules
   - internal reviews, unpublished results marked as such
   - anything export controlled

- Any principles or policy should be the same/similar for conventional tools, and the same for all forms of internal documentation
  - Technical or analysis notes
  - Software, merge requests, issues
- Note, SI produces English language intended for SI consumption, and intentionally not for human consumption. So, when you give it as-is to another human, your expectations should be tempered!

Discuss!