Full-cycle Project Achievement Archiving Specification V1.0

Project: Wallet–RPC Privacy Leakage Measurement (Empirical Study)
Version: V1.0 (Milestone 1 Release)
Scope: Defines standardized GitHub repository framework and unified full-lifecycle achievement management rules for the project, aligned with CS6290 course requirements and team collaboration practices.

1. Core Archiving Principles

All project achievements must follow these core principles, with flexible iteration allowed for subsequent milestones:

1. **Reproducibility & Verifiability**: All archived content must be traceable, reproducible, and fully matched with the course's evidence-based scoring rules.
2. **Course Compliance First:** All mandatory content required by CS6290 (individual evidence packs, AI usage transparency, milestone deliverables) has the highest archiving priority.
3. **Iterative Compatibility:** The specification supports version updates along with milestone iterations, with all historical versions retained for traceability.
4. **Secure Desensitization:** No unmasked sensitive data (full private RPC URLs, real user wallet addresses, private keys) is allowed in the public repository.
5. **Unified Collaboration:** Consistent naming and storage rules for the whole repository to reduce team collaboration costs and facilitate cross-role content integration.

2. Standardized Repository Core Framework

This framework is fully compatible with the existing project repository structure, with only core first-level directories defined (subdirectories can be flexibly adjusted by

each role according to actual needs):

Core Directory	Primary Archiving Purpose
src/	Core runnable code of the RPC measurement harness, including all functional modules developed by the team
configs/	Reproducible experiment configuration files, scenario definitions, and test-related parameter files
docs/	All project documents, including specification documents, project proposals, threat models, pre-research notes, and milestone reports
logs/	Desensitized experimental raw logs and structured metric summary results generated by the measurement harness
evidence/	All team members' individual evidence packs for each milestone, plus verifiable supplementary materials (screenshots, validation records)
ai_transparency/	Unified archiving of all team members' AI usage records, aligned with the course's mandatory disclosure requirements
archive/	Frozen full deliverable packages for each milestone after submission, and historical versions of core documents

3. Milestone-based Archiving Rules

Core mandatory archiving content for each milestone, aligned with the project's phased delivery plan：

Milestone	Mandatory Archiving Content
M1 (Project	Core project documents (proposal, scope definition, threat model

Milestone	Mandatory Archiving Content
Proposal & Planning)	v1.0, specification documents)2. Runnable baseline measurement harness code and reproducible experiment configs3. All team members' M1 individual evidence packs and AI usage records4. Frozen M1 full deliverable archive package
M2 (Mid-term Empirical Progress)	Iterated project documents and updated threat model2. Full desensitized experimental logs, metric results, and phased analysis outputs3. All team members' M2 individual evidence packs and updated AI usage records4. Frozen M2 full deliverable archive package
M3 (Final Delivery)	Final version of all project documents, complete experimental dataset, and final analysis results2. Final project report, empirical study report, and mandatory AI collaboration appendix3. All team members' M3 individual evidence packs and full-cycle AI usage records4. Frozen final full deliverable archive package and complete historical version archive

4. Mandatory Compliance Rules

1. **AI Transparency (Course Mandatory):** Each team member must submit a complete AI usage record for each milestone, including tool name, usage scenario, accepted output, and 1 rejected output with clear reasons. All records must be archived in the ai_transparency/ directory.

2. **Data Desensitization:** All experimental logs, configuration files, and documents must be desensitized before archiving. Only demo addresses are allowed in the public repository, and private RPC URLs must be masked.

3. **Version Management:** All core documents and code must have clear version numbers, and each milestone update must retain the previous historical version.

4. **Evidence Consistency:** All content stated in individual evidence packs must have corresponding archived files in the repository to ensure full verifiability.

5. Pre-submission Validation Checklist

Before each milestone submission, the following checks must be completed:

· All mandatory deliverables for the current milestone are fully archived in the corresponding directory

· All content in individual evidence packs has corresponding verifiable files in the repository

· No unmasked sensitive data exists in the repository

· All team members' AI usage records for the current milestone are completely archived

· The archived content is fully consistent with the current version of this specification

6. Role-based Archiving Responsibilities

Role	Core Archiving Responsibility
Project Management & Archiving Lead (Owner of this Specification)	Responsible for the maintenance, version iteration and compliance review of this archiving specification; responsible for the final compliance check of the repository structure and archived content before each milestone submission; responsible for coordinating the archiving progress of all roles and ensuring the integrity of milestone deliverables
Developer / Tool Developer	Responsible for archiving the core runnable code of the RPC measurement harness, reproducible experiment configuration files, desensitized experimental logs and related code documents into the corresponding directories; ensuring the archived code is runnable, consistent with the experimental results, and annotated clearly
Document & Specification Lead	Responsible for archiving all project core documents (including project proposal, scope definition, technical specification documents, milestone reports, presentation slides) into the corresponding directories; ensuring the consistency of document versions, standardization of format,

Role	Core Archiving Responsibility
	and alignment with the project's phased progress
Security & Threat Model Lead	Responsible for archiving the project's threat model, privacy risk list, validation scheme, verification records and test results into the corresponding directories; ensuring the archived content is traceable, verifiable, and consistent with the project's privacy measurement objectives
Research & Data Analysis Lead	Responsible for archiving pre-research notes, literature excerpts, metric design documents, experimental data analysis results, and data visualization materials into the corresponding directories; ensuring the one-to-one correspondence between analysis results and original experimental logs, and the reproducibility of research conclusions
All Team Members	Responsible for submitting personal individual evidence packs and complete AI usage records for each milestone to the corresponding directories; strictly complying with the requirements of this specification for personal work archiving