

GSCP

GenAI Security Certified Professional

CANDIDATE HANDBOOK

Read this before you press Begin. It covers what you need, the rules you agree to, what happens during the exam, and what happens after you submit.

4 hours

Exam length

75%

Pass mark

1 day

Examiner review

No expiry

Attempts and credential

BEFORE THE EXAM

What you need

Computer	A desktop or laptop
Browser	A current desktop version of Chrome, Edge or Firefox, so the platform can record your screen
Integrity	Screen recording and integrity checks. Not proctored.
Time	4 hours you can keep free
Connection	Stable enough to keep sharing your screen

Booking

There is nothing to book. Once you own an attempt, you start whenever you are ready. An unused attempt does not expire.

Accommodations

If you need an accommodation, describe it in the exam agreement before you press Begin. An examiner reviews every request. Making a request does not change your exam clock.

THE AGREEMENT

You accept the rules before the clock starts

Each attempt starts with an exam agreement. You confirm that you have read it, that you will do the exam on your own with no AI assistance, and that you agree to your screen being recorded and reviewed by an examiner. The clock does not start until you press Begin.

DURING THE EXAM

The rules

Allowed

- A browser
- A text editor and a terminal
- Your own notes
- Public references that you read yourself

Not allowed while the clock runs

- AI assistants, copilots, chatbots or autonomous agents of any kind, including AI built into your browser, editor or terminal
- Help from any other person
- Copying, publishing or sharing the exam targets, their content or your solutions, during or after the exam

The exam targets are the only AI systems you interact with.

The clock

Once you press Begin, the 4-hour clock runs and cannot be paused. Your targets stay available until it ends. When time runs out, your attempt is submitted automatically with whatever you have completed.

Working the target

You get a live AI application. For each vulnerability you exploit, capture the evidence the exam asks for and write a few lines, in your own words, on how you found it. The platform checks your evidence against the live target.

Screen sharing

Share your entire screen, not a single window or tab, and keep sharing for the whole exam. If sharing stops, resume it straight away. Gaps in the recording are visible to the examiner and can lead to the attempt being voided.

AFTER YOU SUBMIT

Results, review and the credential

- 1 Your score**
Shown as soon as you submit.
- 2 Examiner review**
A named examiner reviews every passing sitting, within 1 business day. A passing score does not issue a credential on its own.
- 3 Your credential**
Issued when the examiner releases the result. It carries a unique ID and resolves to a public verification page showing the holder, the credential, its status and its issue date. Scores stay private.

If you do not pass

You get a domain-level breakdown of where you fell short. It never shows the answers or the exploit paths. One free retake is included, on freshly randomized targets. Further attempts are paid.

If the rules were broken

If the examiner finds that the agreement was broken, the attempt is voided. No credential is issued and the attempt counts as used.

Validity

The credential does not expire. Because the field moves quickly, we recommend recertifying every 24 months.

Confidentiality

Do not copy, publish or share the exam targets, their content or your solutions, during or after the exam.

Questions, or something stopped you during the exam

support@genaisecuritylab.com

The exam agreement you accept before each attempt is the binding version of these rules. This handbook describes version 1.0 of the GSCP exam; the current version is on genaisecuritylab.com.