cross-chapter-anthropic-cyber-use-citation.md

1,311 words · ~6 min read

Anthropic Acceptable-Use Cyber-Research Exception: Canonical Citation Reference

Overview

Field	Value
Tier	cross-chapter reference
Type	Policy citation document -- NOT a course module
Lab	None
Rubric	None
Audience	Academy operators, curriculum authors, cohort-lab facilitators
Status	Canonical; version 1.0 (2026-05-07)
Syntax validated	Manual (no Anthropic AUP parser; AUP URL verified HTTP 200 at time of authoring)
Paired pages	Forward-pointed from each handout performing offensive-reproduction work
Policy source of truth	https://www.anthropic.com/legal/aup (link; do not paraphrase inline)

This handout is a **policy citation reference**, not a lesson. The central artifact is the footnote convention in §3: a one-line forward-pointer pattern that downstream handouts embed in their document overview section. When the Anthropic acceptable-use policy updates, this handout is the single point of revision; downstream handouts inherit the update via the forward-pointer.

---

§1 What this handout covers

This handout documents the Anthropic acceptable-use cyber-research exception that authorizes Virtus Cyber Academy's offensive-reproduction work. That work includes CVE-trigger PCAP synthesis on academy-isolated test ranges, binary-diff analysis against pre-patch vulnerable application builds, and exploitation-primitive demonstration in cohort labs.

Each handout in the academy's offensive-reproduction family carries a one-line forward-pointer footnote in its document overview section citing this document. The footnote tells readers -- students, auditors, and instructors alike -- where the policy authorization is documented and what its scope is.

This handout does not cover the full Anthropic acceptable-use policy. It covers only the cyber-research exception relevant to the academy's curriculum work.

---

§2 The policy framework

§2.1 Anthropic acceptable-use policy

The canonical policy lives at:

https://www.anthropic.com/legal/aup

Cite the URL; do not paraphrase the policy text inline. Paraphrasing risks accidental misrepresentation; the link is the source of truth and remains authoritative as Anthropic updates the policy.

Anthropic's acceptable-use policy permits security research, educational security work, and academic offensive-security curriculum when conducted within defined boundaries. The policy explicitly distinguishes between legitimate security research (permitted) and unauthorized offensive operations against third-party systems (prohibited). The academy's work falls within the permitted category subject to the conditions in §2.2 and §2.3 below.

If you need to cite a specific clause or section number for a formal audit, retrieve the current policy text from the URL above and note the section at the time of citation. Policy section numbering can shift across revisions; the URL is durable.

§2.2 Cyber-research exception scope

What the exception covers:

- Academic offensive-security curriculum: teaching students to recognize, reproduce, and defend against disclosed CVE classes using academy-owned materials on academy-controlled infrastructure.
- Reproduction of publicly disclosed CVEs against academy-owned vulnerable binaries (pre-patch builds, deliberately vulnerable VMs, or controlled Docker containers under academy administration).
- PCAP synthesis on academy-isolated test ranges: generating or capturing traffic that triggers known vulnerability patterns for instructional purposes.
- Exploitation-primitive demonstration in cohort labs: walking students through the mechanics of a disclosed exploit against an academy-owned target in a supervised, isolated lab environment.
- Binary-diff analysis: comparing pre-patch and post-patch application binaries to identify the patched code path and reconstruct the vulnerability surface for curriculum use.
- Security research that produces published curriculum, handouts, or lab materials for the academy.

What the exception does NOT cover:

- Live offensive operations against any system not owned and administered by the academy.
- Any activity that violates applicable law (Computer Fraud and Abuse Act, CFAA; equivalent jurisdiction-specific statutes).
- Any activity that violates third-party acceptable-use agreements (hosting providers, cloud platforms, software vendors).
- Sharing exploit code, tooling, or methodology outside the academy's cohort context in ways that could enable unauthorized access.
- Attacks against production systems, even if the academy is a client or user of those systems.

The boundary is ownership and authorization: academy-owned targets in academy-controlled infrastructure, for curriculum use, in authorized lab sessions.

§2.3 Account architecture

The academy operates under a dual-account model that separates general Claude work from cyber-research work:

Account	Email	Role	Exception status
munsonj	munsonj@gmail.com	General legacy account; non-offensive work	General cyber-use approval (legacy)
munsonj2.0	munsonj2.0@gmail.com	Academy-designated account	Cyber-research exception (approved 2026-05-03)

All offensive-reproduction curriculum work -- CVE-trigger PCAP synthesis, binary-diff lab authoring, exploitation-primitive demonstrations, range administration -- is conducted under **munsonj2.0@gmail.com**. This account carries the explicit Anthropic cyber-research exception approval granted 2026-05-03.

The separation provides a clean policy boundary: the exception is scoped to the account, which is scoped to the academy's offensive-reproduction work. Cross-contamination (running offensive-curriculum prompts from the general account, or vice versa) undermines the policy boundary and should be avoided.

Implementation note on switching: Account re-login is laptop-wide and affects all active Claude sessions simultaneously. Coordinate session switches with active orchestrators to avoid mid-task account mismatches. Verify the current account via `/status` on an idle Claude session before starting offensive-reproduction work.

§2.4 Discipline reminders

These practices are expected across all academy offensive-reproduction work. They are not bureaucratic overhead; they are the discipline that makes the exception defensible.

`--authorized-by` annotation. Every cohort-lab exercise, script, or automated harness step that invokes an offensive-reproduction action carries an `--authorized-by` annotation in its configuration or header block. The annotation cites this handout by filename. Example:

```
# --authorized-by: handouts/cross-chapter-anthropic-cyber-use-citation.md
# Scope: CVE-2026-5402 TLS ECH heap-overflow reproduction on academy fwlab
container
```

Cohort-student scope. Students operate exclusively against academy-owned, deliberately vulnerable targets on academy-isolated infrastructure. The lab harness (`fwlab` container, isolated test-range VM, or equivalent) enforces this boundary at the network layer. Students do not have credentials or network routes to production or third-party systems from within lab sessions.

Provenance metadata. Each PCAP capture, binary artifact, or exploit output published as curriculum material carries provenance metadata: the CVE it targets, the academy infrastructure it was generated on, the date, and the authorized session or operator that produced it. The sidecar metadata convention is documented in the range administration guide (forthcoming; §4 forward-pointer).

Lab-session authorization. Cohort-lab sessions that include offensive-reproduction exercises are documented in advance (lesson plan, lab worksheet, or operator brief) with explicit scope boundaries. Unplanned offensive-reproduction is not authorized under the exception.

---

§3 Citation footnote convention

§3.1 The pattern

Any handout that performs or supports offensive-reproduction work places the following one-line footnote in the §0 overview, as a separate row or as a trailing note after the register table:

```
[Authorized under Anthropic acceptable-use cyber-research exception; see handouts/
cross-chapter-anthropic-cyber-use-citation.md for policy details and academy
provenance.]
```

This is the exact string. Do not paraphrase it. The filename must be exact so that tools and auditors can grep for it and confirm coverage.

§3.2 Where to place it

In the document overview section of any handout that:

- Presents exploitation-primitive rule templates or PCAP synthesis procedures.
- Documents binary-diff methodology against pre-patch vulnerable builds.
- Describes or includes CVE-trigger lab harness configuration.
- Contains Suricata, Snort 3, Zeek, or YARA patterns derived from CVE reproduction analysis.
- Describes or includes proof-of-concept code or exploit primitives for disclosed CVEs.

If the handout only describes or explains a CVE without providing operational reproduction steps, the footnote is optional but encouraged.

§3.3 Worked example

Below is an illustrative document overview section for a hypothetical offensive-reproduction handout showing the footnote inserted correctly:

```
## Overview

| Field | Value |
|---|---|
| **Tier** | offensive-reproduction reference |
| **Type** | Per-CVE PCAP synthesis lab guide |
| **Lab** | fwlab container; academy test-range only |
| **Audience** | ADV-101 cohort; SEC-101 facilitators |
| **CVE** | CVE-2026-5402 |
| **Syntax validated** | Manual; no live Wireshark binary available in authoring
environment |

[Authorized under Anthropic acceptable-use cyber-research exception; see handouts/
cross-chapter-anthropic-cyber-use-citation.md for policy details and academy
provenance.]
```

The footnote sits after the table, as a standalone bracketed line. It is not a table row. It does not need a heading.

§4 Cross-references: handouts requiring the footnote

The following existing and in-flight handouts perform offensive-reproduction work and should carry the §3 footnote in their document overview section.

§4.1 Existing handouts (follow-on retroactive pass)

Handout file	Work type	Footnote status
`handouts/cve-lab-wireshark-rce-quartet-2026-05.md`	CVE reproduction lab harness; exploit-primitive taxonomy	Needs footnote
`handouts/cve-suricata-rules-reference-wireshark-quartet-2026-05.md`	CVE-derived Suricata rule templates	Needs footnote
`handouts/cve-snort3-rules-reference-wireshark-quartet-2026-05.md`	CVE-derived Snort 3 rule templates	Needs footnote
`handouts/cve-class-zip-slip-pattern.md`	Zip-slip exploitation pattern (CWE-22)	Needs footnote

§4.2 In-flight handouts (apply footnote at authoring time)

Handout file	Work type	Footnote status
`handouts/re-101-cve-quartet-binary-diff-lab-cluster.md`	Binary-diff lab cluster; pre-patch vs post-patch Wireshark builds	Apply at authoring time

§4.3 Forthcoming handouts (forward-pointer flag)

Asset type	Footnote requirement
Per-CVE captures sidecar metadata files	Apply footnote or equivalent `--authorized-by` annotation at creation time
Range administration guide	Apply footnote; the guide documents academy test-range infrastructure used for all offensive-reproduction work
Per-CVE YARA rule reference handouts (§8.3 supplement in Snort 3 sibling)	Apply footnote at authoring time
Cohort-lab Snort 3 deployment recipe handout	Apply footnote at authoring time

---