# ACADEMY ACCEPTABLE USE POLICY

**cyber-sec.si** and **academy.cyber-sec.si**

Version: 1.1

Last updated: 7. september 2025

# TABLE OF CONTENTS

**Company:** CYBER-SEC, informacijska in kibernetska varnost, d.o.o.
**Registered office:** Tolstojeva ulica 41, 1000 Ljubljana, Slovenia
**VAT ID:** SI89630777
**Company Registration Number (Matična številka):** 9827021000
**Contact for violations / security / legal:** academy@cyber-sec.si
**Effective date:** 7 September 2025
**Version:** 1.0

## 1. Purpose and Scope

This Acceptable Use Policy (the "**Policy**") defines prohibited and inappropriate uses of the services, systems, and resources provided or operated by **CYBER-SEC, d.o.o.** ("**CYBER-SEC**"), including (without limitation): websites, learning platforms, labs, exercises/challenges, academy content, live events, servers, networks, and related infrastructure (collectively, the "**Platforms**" or "**Services**"). The Policy applies to all users, participants, customers, employees, contractors, and visitors (collectively, "**Users**").

## 2. Acceptance of the Policy

By accessing or using the Platforms, you agree to comply with this Policy and all applicable laws. If you do not agree, you must not use the Platforms.

This Policy forms part of the contractual framework for using the Platforms and must be read together with CYBER-SEC's Privacy Policy and General Terms.

## 3. Changes to the Policy

CYBER-SEC may update this Policy from time to time. Changes become effective upon publication of the updated version on official communication channels or the Platforms. Continued use after publication constitutes acceptance of the changes.

## 4. Principles of Responsible Use Privacy by design and by default (GDPR Arts. 5 and 25).

Use of the Platforms must be lawful, ethical, safe, and aligned with internet community best practices. The following guidelines and examples of prohibited conduct are illustrative and not exhaustive.

## 5. Prohibited, Harmful, or Offensive Use / Content

You must not use the Platforms—nor encourage, induce, or instruct others to use them—for:

- **Illegal or fraudulent activities:** Activities that are unlawful or infringe upon the rights of others (e.g., phishing, pharming, scams, "get-rich-quick" or pyramid schemes, identity theft), including distribution of child sexual abuse material or other criminal content.

- **Intellectual property violations:** Infringement or misappropriation of copyrights, patents, trademarks, trade secrets, or confidential information of CYBER-SEC or third parties.
- **Offensive or inappropriate content:** Defamation, obscenity, abuse, hate speech, invasion of privacy, or other content that is reasonably objectionable or harmful (including depictions of non-consensual sexual acts or bestiality).
- **Harmful code:** Distributing or intentionally introducing viruses, trojans, worms, time bombs, spyware, or any other malicious/harmful code or technologies.

## 6. Security Violations

You must not compromise the security or integrity of any system (a "**System**"). Prohibited actions include, without limitation:

- Gaining unauthorized access to, attempting to exploit, or testing the normal operation/security of networks, systems, devices, or data;
- Activities that disable or degrade the Platforms or others' use of the internet (e.g., denial-of-service attacks);
- Intercepting, monitoring, or spidering data/communications on systems not owned by you without explicit authorization;
- Attempting to obtain others' credentials or access; redirecting or intercepting communications;
- Circumventing usage restrictions (e.g., quotas, access or storage limits) by manual or automated means;
- Operating open proxies, open mail relays, or open recursive DNS servers;
- Forging TCP/IP packets, email headers, or other metadata regarding message origin/tracking (lawful use of pseudonyms or anonymous remailers, where compliant with law, is not prohibited).

## 7. Email or Messaging Abuse

You must not send or enable the sending of **unsolicited bulk messages** (spam), advertisements, or solicitations, including manipulating message headers or misrepresenting sender identity without the sender's explicit consent. Collecting responses to messages that violate this or others' acceptable use policies is prohibited.

## 8. Identity Deception and Fraud

Prohibited conduct includes:

- Sending messages or engaging in electronic communications using another person's name or address to deceive;

- Misrepresenting your identity (e.g., manipulating source IP addresses or header forgeries);
- Concealing or falsifying identity in connection with use of the Platforms.

## 9. Special Rules for Security Testing, Labs, and Education

- Security testing, competitions, exercises, or labs made available by CYBER-SEC are **permitted solely** within the scope, boundaries, and targets **explicitly** defined by CYBER-SEC (or the customer) and **never** beyond those limits.
- **Prohibited:** attacks, scans, or any testing of targets **outside** the approved ranges; attacks on third-party production systems; disrupting other participants' services; exfiltrating or publishing solutions/flags without permission.
- If you participate in a commissioned security test for a client, you must have **written consent and scope** (e.g., Statement of Work, Rules of Engagement). Any deviation requires prior written approval.
- **Responsible vulnerability disclosure:** Report potential vulnerabilities discovered on the Platforms or at clients only through channels designated by CYBER-SEC, and do not publish details until appropriate remediation is in place or otherwise agreed.

## 10. Security and Privacy

- Users are responsible for safeguarding their credentials. Account sharing is prohibited.
- Processing of personal data is governed by CYBER-SEC's **Privacy Policy** (separate document), available at https://cyber-sec.si/politika-zasebnosti/. Users must comply with the GDPR and applicable laws of the Republic of Slovenia.

## 11. Monitoring and Enforcement

CYBER-SEC may investigate suspected violations of this Policy, remove or disable access to content or resources that violate this Policy or other agreements, and **immediately and without prior notice** suspend or terminate access/use of the Platforms. CYBER-SEC may report suspected unlawful activities to competent authorities and cooperate with them (including disclosing relevant data within the limits of applicable law).

## 12. Reporting Violations

If you observe a violation of this Policy or a vulnerability, **notify us immediately** at: academy@cyber-sec.si. Please include a description, time, scope, and any evidence (do not send sensitive data unnecessarily).

## 13. Limitation of Liability

CYBER-SEC is not responsible for User content or the way Users use the Platforms. The Platforms are provided "as is," without additional warranties, to the extent permitted by law. In no event will CYBER-SEC be liable for indirect, special, incidental, or consequential damages, loss of profit, or data arising from the use or inability to use the Platforms.

## 14. Governing Law and Jurisdiction

This Policy and any disputes arising out of or in connection with it are governed by the **laws of the Republic of Slovenia** and, where appropriate, the **law of the European Union**. The competent courts in Ljubljana shall have jurisdiction, unless otherwise required by mandatory provisions.

## 15. Severability and Non-Waiver

If any provision of this Policy is held invalid or unenforceable, the remaining provisions will remain in full force and effect. Failure to enforce any right does not constitute a waiver of that right.

## 16. Contact

For questions regarding this Policy or requests related to your use of the Platforms, contact:

**CYBER-SEC, d.o.o.**

Tolstojeva ulica 41, 1000 Ljubljana, Slovenia

Email: academy@cyber-sec.si

Website: https://cyber-sec.si/