WARZONE

ONE PLATFORM ALL CYBER

Privacy Policy and Terms of Service

WARZONE (One Platform All Cyber)

Privacy Policy and Terms of Service

LAST UPDATED ON: 28/10/2025

Overview

This Privacy Policy and Terms of Service outlines how WARZONE (One Platform All Cyber) ("we," "us," or "our") platform collects, uses, and shares information when you use our service, including our marketplace services. These services include, but are not limited to, hosting Capture The Flag (CTF) events, scenarios, labs, certifications, and cyber ranges. By using our platform, you agree to comply with the terms of this Privacy Policy and Terms of Service.

Legal Disclaimer and Limitations of Liability

WARZONE (One Platform All Cyber) provides cybersecurity training and educational resources to help users enhance their skills and advance their careers. However, WARZONE (One Platform All Cyber) is not responsible for how users apply the knowledge, techniques, or tactics learned on the platform. Any misuse of such skills for illegal or unauthorized activities is strictly prohibited, and users bear full responsibility for their actions outside the platform. WARZONE (One Platform All Cyber) disclaims any liability for the consequences of improper or unlawful use of its training materials.

Accuracy of Verification: While we make every effort to verify the accuracy of the information provided by users, we are not responsible for any errors or inaccuracies in the submitted documents, including passport images.

Use of Passport Information: The passport image you submit is only used for the purpose of **identity verification** and is deleted immediately after the decision has been made.

Accuracy of Verification

WARZONE (One Platform All Cyber) provides cybersecurity training and educational resources to help users enhance their skills and advance their careers.

- Responsibility: We are not responsible for how users apply knowledge or tactics learned on the platform. Misuse for illegal/unauthorized activities is strictly prohibited.
- User Accountability: Users bear full responsibility for actions outside the platform.
- Disclaimer: We disclaim liability for the consequences of improper/unlawful use of training materials.

Information We Collect

Personal Information

- Name
- Email address
- Contact information
- User-generated content (e.g., challenge submissions, comments)
- Device information (e.g., browser type, operating system)

Additional Information:

Personal & Payment Information

- The platform collects and processes:
- Payment info, billing address, and transaction history.
- Handled by a third-party service provider.

Passport Image Submission

- Required for identity verification.
- Must comply with Passport Image Submission Guidelines.
- False or misleading information is considered fraud and may lead to:
- Account suspension or termination without notice.
- Legal consequences under applicable laws.
- Users must cooperate in good faith with verification requests.

Data Collected

- Usage history, subscription info, and account preferences.
- Cookies and tracking technologies are used for:
- Monitoring usage
- Saving preferences
- Improving services

Fraud Policy

- Providing false or misleading information is strictly prohibited.
- The platform reserves the right to:
- Verify information at any time.
- Request additional documentation for verification.

KYC/CDD Policy:

To ensure compliance with applicable laws, regulations, and to maintain the integrity of our platform, we require accurate and truthful information from all users when filling out any forms on our platform. This includes, but is not limited to, the following scenarios:

- Account Sign-Up
- Login Details
- Payment information
- Purchases or Transactions
- Participation in Events, Labs, or Competitions

"Providing false, inaccurate, or misleading information is strictly prohibited and will be considered an **act of fraud.** Any such violations may result in suspending or terminating your account without prior notice. Also, fraudulent activities may be subject to legal consequences according to applicable laws. We reserve the right to verify the accuracy of the information you provide at any time and may ask for additional documentation for identity verification purposes. By using our platform, you agree to cooperate with any such requests in good faith".

Age Limitation

WARZONE does not allow anyone younger than **18 years old** unless a written parental or legal guardian consent is provided through our relevant consent form. All information provided for users under 18 will be processed and stored in compliance with applicable laws, with additional safeguards to protect minors data.

How we use your information

- To provide and maintain our Service In connection with a merger, acquisition, or sale of assets
- To personalize users experience
- To communicate with you, including responding to inquiries and providing updates
- To analyze usage of the Service and improve our offerings
- To comply with legal obligations
- To ensure the security and integrity of our platform, including fraud detection and prevention

Sharing of Your Information

We may share your information in the following circumstances but not limited to:

- With our service providers, who assist us in providing the Service.
- With our affiliates and partners, for the purposes described in this document.
- In response to a legal request or to comply with applicable laws, regulations, or governmental requests.
- In connection with a merger, acquisition, or sale of assets
- To communicate with you, including responding to inquiries and providing updates
- With professional advisors such as auditors or legal consultants to ensure compliance and operational efficiency

Marketplace Specific Information:

This section outlines how we handle data related to WARZONE Marketplace services, including but not limited to hosting Capture The Flag (CTF) events, scenarios, labs, and cyber ranges. By using our marketplace services, you agree to the following terms:

- Account Requirements: To access and purchase products and services from our marketplace, customers are required to create an account. This account will store your purchase history, preferences, and other relevant details to facilitate your engagement with our services.
- Data Collection: We collect and process personal data when you use our marketplace services. Additional data collected includes but is not limited to:

Payment Information: Billing address, and transaction history (processed by a third-party service provider)

Usage Data: Website activity, including event participation.

WARZONE Coins Usage *(Details of purchases and transactions using our in -platform currency)*

- *WARZONE coins: All purchases on our marketplace are made using WARZONE Coins. These coins can be purchased, earned during events, or acquired through other methods and are used for purchasing digital products, services, and event participation. Refunds, if applicable, will be issued in WARZONE Coins after validation by our support team.*

- *No Resale or Sharing of Products: Products and services purchased through the WARZONE market place are licensed for personal use only. Reselling or sharing any digital content is prohibited and may result in account suspension or termination.*

User-Submitted Blog Content

When you submit blog articles to WARZONE for publication, please be aware that once your submission is reviewed and approved by the WARZONE Staff, the article will become publicly accessible on our platform. This means it may be indexed by search engines and become discoverable through public search results.
By submitting content, you agree not to include:

- Personal Information.
- Sensitive Data.
- Content that may violate this Privacy Policy or our Terms of Service.

WARZONE is not responsible for any personal or sensitive information you voluntarily disclose within your article. We strongly advise all contributors to review their submissions carefully to ensure compliance and to protect their own privacy and security.

Premium Subscription and Payment Terms

WARZONE premium subscription is offered at a fixed price displayed on our platform and payable using WZC, our in-house currency. To maintain your subscription, you must have a sufficient WZC balance on the renewal date.

Subscriptions automatically renew on the 1st of each month. If your WZC balance is insufficient at the time of renewal, your subscription will be canceled automatically.

You are free to cancel your subscription at any time, and you can also resubscribe whenever you choose. For detailed information on the features and benefits included with the premium subscription, please visit the Shop section on the portal.

Bug Bounty Policy

ELIGIBILITY AND ACCESS

- Participation in the Bug Bounty Program is limited to individuals who are 18 years of age or older. WARZONE requires that all bounty participants verify their identity via our KYC process (Settings > Verification) or maintain accurate, truthful profile information, including full legal name, age, and payment details.
- The Bug Bounty section is not publicly visible on the portal by default and is accessible only to eligible users.
- Submissions made with falsified or incomplete identity data may result in denial of rewards, delayed processing, or permanent exclusion from the program.

DATA ACCESS AND RESPONSIBLE TESTING

- Researchers are expected to act in good faith and must not access, exfiltrate, or destroy any user data, documents, or internal content while testing. Proof of Concept (PoC) demonstrating the vulnerability is sufficient.
- WARZONE prohibits the use of discovered vulnerabilities to extract real data or harm system integrity. Violations may lead to legal action and permanent bans.

PAYMENT TERMS AND PROCESS

- Bounty rewards, where applicable, are processed in U.S. Dollars (USD) and are subject to local laws, regulations, and ethics rules.
- You are responsible for the tax consequences of any bounty you receive, as determined by the laws of your country. Additional fees may apply, such as currency conversion or other transaction-related charges.
- Payments are only made to accounts that have completed identity.
- The payment window is set by the entity and may be extended due to various operational or legal factors.
- If your Warzone account contains inaccurate, incomplete, or falsified information, your payment may be delayed, rejected, or lead to disqualification from current and future programs.
- WARZONE does not process payments to users in countries affected by export restrictions, sanctions, or other legal limitations.
- To process Bug Bounty rewards, WARZONE may collect and use your verified identity details (e.g., name, country, payment info) solely for compliance with international regulations and legal payout procedures.
- WARZONE will not disclose any personal data unless required by law or in cases of fraud or abuse.

REWARD POLICY

- Not all entities participating in WARZONE's Bug Bounty Program offer monetary rewards.
- The decision to award a bounty, and the amount, is entirely at the discretion of the entity and the rewards are granted only if:
  - The vulnerability is valid and previously unreported.
  - You are the first to report the issue.
  - Your conduct and submission comply with these policies and entity scope and rules.

RESEARCHER CONDUCT & GUIDELINES

Researchers must adhere to the following principles:

- Operate Ethically: Never exploit a vulnerability for personal gain or access unauthorized data.
- No Data Exfiltration: Proof of concept is sufficient. Extracting data (e.g., databases, internal documents) is strictly prohibited and may result in legal action.
- Maintain Confidentiality: Do not disclose program details or vulnerabilities externally without express written consent from the entity.
- Report Responsibly: Submit vulnerabilities with clear, reproducible steps or a working proof-of-concept. Lack of detail may cause processing delays.
- Respect the Rules: All actions must comply with WARZONE's Privacy Policy, Terms of Service, and each entity's specific program scope and rules.

SAFE BOUNTY HUNTING

- All personal information on your WARZONE account must be accurate, including your full legal name and age.
- Reports from unverified or non-compliant users will be rejected, and participation may be revoked.
- WARZONE aims to protect responsible Researchers, but full cooperation with these guidelines is essential for support in complex disclosure situations.

PUBLIC RECOGNITION

- Researchers may receive public recognition on their WARZONE profile.
- Recognition is granted only if:
  - You are the first reporter of a validated issue.
  - The vulnerability is confirmed.
  - All rules and guidelines have been followed.

ENTITY RESPONSIBILITIES

Entities creating a program are expected to:

- Prioritize Security: Resolve issues promptly and transparently.
- Respect Researchers: Acknowledge and credit valid contributions.
- Reward Appropriately: Offer incentives when possible and appropriate.
- Act Fairly: Refrain from punitive or retaliatory actions against good-faith researchers.

VULNERABILITY DISCLOSURE & MEDIATION

- All vulnerabilities must remain confidential between the Researcher and the Entity.
- Researchers are prohibited from disclosing or discussing the details of any vulnerability without explicit written permission from the involved entity.
- Public disclosure without consent may lead to legal consequences and immediate suspension.
- If no agreement is reached between the two parties, either may request a mediation process. WARZONE will act as a neutral third party to assess and resolve the issue fairly.
- In the event of duplicate reports, the submitting researcher will be shown the original validated report for transparency.

SCOPE AND RULES

- Each Entity defines its own Bug Bounty Program scope, rules, and eligible testing assets.
- Researchers must read and comply with the specific program rules prior to submission.

SAFE TESTING EXPECTATIONS

Researchers must:

- Never harm, disrupt, or degrade WARZONE or entity systems.
- Avoid any form of DDoS, brute-force, or automated testing unless explicitly allowed by the entity's program rules and scope.
- Never perform phishing, social engineering, or attacks on others unless explicitly allowed by the entity's program rules and scope.
- Only test systems listed in-scope by the entity program.

Intellectual Property Rights:

Users are prohibited from posting or sharing other players information, screenshots of details, or any proprietary elements of the platform without explicit permission of WARZONE (One platform ALL Cyber). This includes any content that might infringe upon the intellectual property rights of others. Violations will be addressed to maintain the integrity and legality of the platform.

Data Security :

We are committed to ensuring the security of our platform and protecting your data. This includes:

- Prohibiting attacks beyond designated infrastructure (e.g., the VPN gateway, CTF platform)
- Restricting flag and hint sharing, sabotage, spoofing, and participant-targeted attacks
- Advising the use of isolated virtual machines for participation.
- Ensuring the security of our platform and promoting fair usage are fundamental principles we uphold. We implement robust measures to safeguard your data against unauthorized access, disclosure, alteration, and destruction. While we strive to maintain the highest standards of security, we acknowledge that no system is entirely immune to risks.
- In the event of any security breaches or unauthorized access, we will promptly take action to secure your data and minimize any potential impact.
- It's important to us that our platform operates with integrity and fairness. Any attempts to exploit or misuse the platform, including hacking, spreading viruses, or other malicious cyber activities, cheating, manipulation of results, or engaging in dishonest behavior, are strictly prohibited. Users found violating these principles may face consequences, including termination and other appropriate actions.
- We also reserve the right to report any suspected illegal activities to the relevant authorities and cooperate with their investigations as necessary.
- We take the security of your passport image and other personal data seriously. Once the verification process is concluded (whether approved or declined), your passport image is immediately deleted from our systems.
- No Third-Party Tools: We do not use any third-party services or external tools for account verification. All passport image verification is handled internally by our staff, ensuring that your data remains secure within our systems.

User Rights:

As a user of WARZONE, you have the right to:

- Access your data.
- Update or correct your data.
- Delete your data upon written request.
- Object to certain processing activities.

Caution: These rights may be subject to limitations in cases where we are required to retain data for legal, regulatory, security, or fraud-prevention purposes. We reserve the right to deny certain requests if they conflict with our obligations under applicable laws or compromise the integrity and security of our platform.

Tracking Technologies:

Our platform utilizes tracking technologies to ensure the security, functionality, and performance of the Service.

- Enhance User Experience: Track and analyze user interactions to personalize and improve the Service based on performance analytics and user feedback.
- Monitor Security: Detect and respond to potential security threats, ensure the integrity of the platform, and prevent unauthorized access.
- Performance Optimization: Analyze system performance and user behavior to identify areas for improvement and optimize overall platform efficiency.
- While these technologies help us provide a better and safer experience, we do not use them for targeted advertising or other marketing purposes. We are committed to safeguarding your privacy and ensuring that any data collected is used solely for the intended purposes described herein.

Inappropriate Content and Data Policy:

Our platform is committed to maintaining a safe and respectful environment for all users. To ensure this, we have established strict guidelines regarding the type of content and data that can be uploaded to our service. This includes, but is not limited to, images, biographical information, full names, and any other personal or sensitive data.

Prohibited Content:

- Obscene or Offensive Material: Content that is violence and Harmful Behavior, pornographic, obscene, vulgar, offensive in nature or any Illegal Activities as deemed by the law.
- Hate Speech: Content that promotes hatred, or discrimination against individuals or groups based on race, ethnicity, religion, disability, or any other characteristic.

Inappropriate Content and Data Policy (Continued):

- Personal and Sensitive Information: Uploading or sharing personal or sensitive information about others without their explicit consent, including but not limited to full names, addresses, phone numbers, and private biographical details.
- Harassment and Bullying: Content that harasses, intimidates, or bullies individuals or groups, including trolling.
- False Information and Misleading Content: Content that spreads false information, misinformation, or disinformation with the intent to deceive or manipulate users
- Intellectual Property Violations: Content that in fringes upon the intellectual property rights of others, including copyright, trademark, and patent violations.
- Spam and Phishing: Content that is spammy, deceptive, or designed to trick users into providing personal information or engaging in fraudulent activities.
- Malware and Malicious Content: Content that contains or distributes malware, viruses, spyware, or other malicious software.

Streaming, Recording & Writeups:

To protect intellectual property and maintain the integrity of WARZONE content, the following streaming, recording and writeup policies apply

1. Courses / Labs:
- Streaming/Recording: Not allowed
- Writeups: Not allowed.

2. Public (Portal-Hosted) Events:
- Streaming/Recording: Not allowed.
- Writeups: Allowed only after the event is concluded.

3. Private (XTENDED-Hosted) Events:
- Streaming/Recording: Not allowed.
- Writeups: Allowed only after the event is concluded and only in invite-only environments (e.g., private Discord groups of a specific entity).

Any violation of these policies may result in penalties, including but not limited to user account bans and/or legal consequences.

Payment processing:

We do not collect, handle, or store your credit card details or any other payment method information. All payments are processed exclusively through a third-party payment gateway. We do not have access to or retain your payment credentials.

Refunds and credits:

If you are eligible for a refund, it will be issued in WZC coins only. No refunds will be provided via the original payment method or in cash unless explicitly stated otherwise.

Certifications Support and requests:

For support related to certification exams, refund requests, or other certification-related inquiries, contact: certifications@siu23.com. Provide your full name, Warzone account name, exam name, exam date, and a clear description of your request to help us respond faster.

Proctoring and exam rules:

All candidates must follow the proctoring guides and exam rules provided prior to the exam. Failure to follow the proctoring instructions (including any pre-exam checks, camera or screen requirements, or identification steps) may result in immediate rejection and an automatic fail for the exam.

Academic integrity and cheating:

Cheating, attempting to cheat, or otherwise violating exam rules will result in a failing grade for that exam. This includes but is not limited to collusion, using unauthorized materials or devices, attempting to impersonate another candidate, and any behavior that compromises exam integrity.

Exam confidentiality and sharing restrictions:

Exam content is confidential and is not shared with third parties. You are strictly prohibited from sharing any exam content, including questions, answers, exam structure, setup, methodologies, or any other information that could lead to content disclosure. You may share general impressions of your experience (for example, “the exam was challenging”), but you must not disclose any details about how the exam is formed or administered.

Consequences of content leaks or violations:

If you leak or attempt to leak exam content or otherwise breach these rules, we reserve the right to cancel any certificates issued to you, suspend or terminate your account, ban you from future certifications, and pursue any additional measures or remedies available under our policies and applicable law.

Name on certificate and identity verification:	We strongly recommend using your real full name on your Warzone account; this is the name that will be printed on your certificate. If you change your name after a certificate is issued, updating the certificate will require an identity verification process that may be lengthy and will require submission of government-issued identification (for example, a passport). Delays or additional verification requirements may apply.
Data Retention:	We will retain personal data for up to five (5) years after account closure or contract termination unless a longer retention period is required by law. Sensitive data collected during KYC verification will be retained for six (6) months post-verification or as required by applicable laws.
International Data Transfers:	Your personal data may be transferred to countries outside your home country. Transfers will comply with international regulations, including GDPR, CCPA, and other applicable laws. Where required, we implement safeguards such as Standard Contractual Clauses (SCCs).
Jurisdiction and Governing Law:	This Privacy Policy and Terms of Service is governed by and construed in accordance with the laws of the United Arab Emirates, specifically the jurisdiction of Dubai. However, we comply with applicable international privacy laws, including GDPR for users within the European Economic Area (EEA) and CCPA for users in California. Any disputes arising out of this Privacy Policy and Terms of Service or the use of WARZONE services will be subject to the exclusive jurisdiction of the courts of Dubai, UAE.
User Consent:	By using our platform, you consent to the collection, processing, and use of your personal data as described in this policy. WARZONE (One Platform All Cyber) ("we," "us," or "our"), owned and powered by SECINTEL Unit. If you do not consent, refrain from using our platform. By using our platform, you agree to abide by our content policies and understand the consequences of violations, including account suspension or legal actions. We strive to ensure a safe and respectful environment for all users.
Changes to Our Privacy Policy and Terms of Service:	We reserve the right to modify this policy at any time. Changes will be effective immediately upon posting on our platform. Users will always have access to the latest version of the Privacy Policy and may be required to explicitly agree to significant updates. “If you have any questions or concerns about this Privacy Policy or our Terms of Service, please contact us at contact@siu23.com. By using WARZONE (One Platform All CYBER) platform and services, which are fully owned and operated by SECINTEL UNIT, Dubai, you acknowledge and agree to our Privacy Policy and Terms of Service, and understand the consequences of violating them. We reserve the right to enforce these consequences at our discretion, without prior notice, to ensure a safe and respectful environment for all users.”