

Free Infrastructure Review Terms

Effective Date: 18.09.2026

These Free Infrastructure Review Terms (“Terms”) govern the free infrastructure review provided by Kernul (“we,” “us,” or “our”), to the organization requesting the review (“Client”).

By expressly accepting these Terms through a checkbox, signed document, or written confirmation, the Client agrees to be bound by them.

1. Eligibility and Authority

The Review is available only to businesses and individuals acting on behalf of a business.

The person accepting these Terms confirms that they:

- are at least 18 years old;
- have authority to bind the Client;
- are authorized to provide Kernul with access to the relevant systems and information;
- have obtained any necessary internal and third-party permissions.

2. Free Infrastructure Review

Kernul will perform a limited, high-level review of the Client’s infrastructure, systems, configurations, documentation, or operational practices (the “Review”).

The specific scope, timing, access method, and expected deliverables will be agreed separately in writing before the Review begins.

Unless expressly agreed otherwise, the Review may include:

- architecture and configuration assessment;
- deployment and delivery processes;
- infrastructure-as-code practices;
- monitoring, logging, and incident-response practices;
- reliability, scalability, and availability considerations;
- security-related observations visible within the agreed scope;
- general recommendations for improvement.

Kernul is not required to investigate systems, environments, or issues outside the agreed scope.

3. Nature and Limitations of the Review

The Review is a limited assessment based on the information, access, and time available to Kernul.

It is not:

- a comprehensive security audit;
- a penetration test;
- a compliance assessment or certification;
- a guarantee that all vulnerabilities, defects, or risks will be identified;
- legal, financial, insurance, or regulatory advice;
- a guarantee of availability, performance, security, or regulatory compliance.

The absence of a finding does not mean that a vulnerability, defect, misconfiguration, or other risk does not exist.

The Client remains responsible for its infrastructure, security controls, backups, regulatory compliance, and decisions made on the basis of the Review.

4. Client Responsibilities

The Client must:

- provide accurate and reasonably complete information;
- identify the systems and environments included in the Review;
- disclose relevant restrictions and safety requirements;
- maintain current and tested backups;
- provide only the minimum access reasonably necessary;
- ensure that access does not violate any law, contract, or third-party right;
- promptly revoke access after the Review;
- avoid providing unnecessary personal or sensitive information.

The Client must not send passwords, private keys, access tokens, or other credentials through the Website's public contact form.

Credentials must be transmitted through a secure method agreed separately by the parties.

5. Access and Changes to Systems

Unless separately agreed in writing, access provided to the Kernul must be read-only.

Kernul will not modify production systems, deploy code, change configurations, delete resources, or perform disruptive testing as part of the Review.

Any implementation, remediation, managed service, or additional technical work requires a separate written agreement.

The Client authorizes Kernul to access and examine only the systems and information included in the agreed scope.

6. Confidentiality

Each party must protect non-public information received from the other party using reasonable care and may use it only for purposes connected with the Review.

Confidential information does not include information that:

- is or becomes publicly available without breach of these Terms;
- was lawfully known to the receiving party before disclosure;
- is received lawfully from a third party without a confidentiality obligation;
- is independently developed without using the other party's confidential information;
- has been effectively anonymized so that the Client, its personnel, and systems cannot reasonably be identified.

A party may disclose confidential information where required by law, provided that it gives advance notice where legally permitted.

These confidentiality obligations continue for 3 (three) years after completion of the Review. Trade secrets must remain protected for as long as they qualify as trade secrets under applicable law.

7. Personal Information

Each party must comply with applicable data protection laws.

The Client must avoid providing personal information that is not reasonably necessary for the Review. The Client confirms that it has a lawful basis for disclosing any personal information included in the Review materials.

Kernul will process personal information only to:

- perform and administer the Review;

- communicate with the Client;
- protect its systems and prevent misuse;
- comply with legal obligations.

Additional information is provided in the Kernul's Privacy notice.

8. Anonymous Case Study

The Client acknowledges that the Review is provided free of charge in consideration for the Kernul's right to prepare, use, and publish an anonymized case study based on its general findings.

Kernul may use the anonymous case study for:

- publication on its Website;
- professional portfolios and presentations;
- educational and informational materials;
- proposals and sales materials;
- social media and other marketing communications.

Kernul may publish and use an effectively anonymized case study worldwide, without time limitation and without payment of royalties or other compensation to the Client.

9. Anonymization Requirements

The case study must not include:

- the Client's name, trading name, logo, trademarks, or domain names;
- names or contact details of the Client's employees or contractors;
- IP addresses, hostnames, account identifiers, or resource identifiers;
- credentials, tokens, keys, secrets, or authentication information;
- specific vulnerabilities that could reasonably be exploited;
- trade secrets or other confidential information;
- personal information.

Kernul must remove or generalize technical and contextual details where their combination could reasonably identify the Client. This may include:

- geographic location;
- exact dates and timelines;
- customer numbers, traffic volumes, revenue, or operational metrics.

Replacing the Client's name with a fictional name is not sufficient if the Client could still reasonably be identified from the remaining information.

10. Client Review Before Publication

Before initial publication, Kernul will provide the Client with a draft of the case study for a confidentiality and identification review.

The Client will have 10 (ten) business days to identify information that:

- identifies or could reasonably identify the Client;
- constitutes confidential information or a trade secret;
- creates a material security risk;
- is materially inaccurate.

Kernul will remove, generalize, or correct information reasonably identified under this section.

The Client may not withhold publication solely because it disagrees with the editorial style or does not wish the anonymized findings to be published.

If the Client does not provide specific objections within the review period, Kernul may publish the case study in accordance with these Terms.

Any later version containing materially new information must undergo the same review process.

11. No Identifiable Marketing Use

The right to publish an anonymous case study does not authorize Kernul to use the Client's identity, logo, trademarks, employee names, quotations, or testimonials.

Any identifiable marketing use requires the Client's separate prior written permission.

12. Ownership and License

The Client retains ownership of materials and information it provides.

Kernul retains ownership of:

- its methodologies, templates, tools, and processes;
- its pre-existing intellectual property;

- the Review report and recommendations created by Kernul;
- the anonymized case study.

Subject to these Terms, Kernul grants the Client a non-exclusive, non-transferable license to use the Review deliverables for the Client's internal business purposes.

The Client grants Kernul a limited license to use materials supplied by the Client only as necessary to perform the Review and create the anonymized case study.

No ownership of either party's trademarks or pre-existing intellectual property is transferred.

13. Retention and Deletion

Kernul will normally delete Client materials, credentials, personal information, and identifiable working records within 30 days after completion or termination of the Review,

unless longer retention is required by law or reasonably necessary to establish, exercise, or defend legal claims.

Access credentials should be revoked immediately after the Review.

Effectively anonymized information and the published anonymous case study may be retained indefinitely because they no longer identify the Client or any individual.

14. No Obligation to Provide Additional Services

The Review does not require either party to enter into any further commercial relationship.

Kernul has no obligation to implement recommendations, correct identified issues, provide ongoing support, or perform additional work unless the parties enter into a separate written agreement.

15. No Warranty

To the maximum extent permitted by law, the Review and its deliverables are provided "as is" and without express or implied warranties.

Kernul does not warrant that the Review will identify every defect, vulnerability, misconfiguration, compliance issue, or operational risk.

The Client is responsible for independently evaluating recommendations before implementing them.

16. Limitation of Liability

To the maximum extent permitted by applicable law, Kernul will not be liable for any indirect, incidental, special, consequential, or punitive loss arising from the Review, including loss of revenue, profits, business opportunities, goodwill, or data.

Kernul's total aggregate liability arising from the Review will not exceed USD 1 (one US dollar).

Nothing in these Terms excludes or limits liability that cannot lawfully be excluded or limited, including liability for fraud or willful misconduct.

17. Suspension and Termination

Either party may terminate the Review by written notice at any time.

Kernul may immediately suspend or terminate the Review if:

- the Client provides unauthorized or unlawful access;
- continuing the Review may create a security or operational risk;
- the Client breaches these Terms;
- the Review would require unlawful or unethical activity;
- the agreed scope cannot reasonably be completed.

Termination does not revoke Kernul's right to publish an anonymous case study based on work already performed, provided that the anonymization and review requirements in these Terms are satisfied.

Sections concerning confidentiality, anonymization, intellectual property, disclaimers, liability, and governing law survive termination.

18. Independent Parties

The parties are independent contractors. These Terms do not create an employment, partnership, agency, fiduciary, or joint-venture relationship.

Neither party may make commitments on behalf of the other.

19. Entire Agreement

These Terms, the agreed Review scope, and any applicable written confidentiality agreement constitute the entire agreement concerning the free Review.

If a separate signed agreement conflicts with these Terms, the signed agreement will prevail.

If any provision is found unenforceable, the remaining provisions will remain in effect.

A failure to enforce any provision does not waive the right to enforce it later.

20. Contact

Questions concerning these Terms may be sent to:

Kernul

Email: hello@kernul.io