SECURITY TERMS OF GREEN:CODE S.R.O.

(the "Terms")

1. Introductory Provisions

1.1 These Terms set out the minimum security obligations of the Supplier when providing Services to the Client (Green:Code s.r.o.) under the Framework Agreement on the Provision of Services (the "Agreement") and individual Partial Agreements. The Terms constitute commercial terms within the meaning of Section 1752 et seq. of Act No. 89/2012 Coll., the Czech Civil Code, and form an integral part of the Agreement.

1.2 Capitalised terms have the meaning given to them in the Agreement (in particular the Client, the Supplier, the Services, a Partial Agreement, an Order).

1.3 The Terms apply to all activities of the Supplier and of any persons engaged by the Supplier in the provision of the Services, to all information of the Client and of the Client's customers to which the Supplier gains access, and to all devices used in the provision of the Services.

1.4 In case of conflict, the Agreement and the relevant Partial Agreement prevail over these Terms. A Partial Agreement or the security requirements of the Client's customer may impose a stricter security regime; they may not relax these Terms unless expressly agreed in the Partial Agreement.

1.5 The Client may provide the Supplier with operational security instructions (Art. 14). An operational instruction applies to the extent it does not conflict with the Agreement, the Partial Agreement or these Terms.

2. General Responsibility of the Supplier

2.1 The Supplier protects the confidentiality, integrity and availability of the information of the Client and of the Client's customers to which it gains access in connection with the Services.

2.2 The Supplier uses the information, access rights, devices and other resources of the Client and of the Client's customers exclusively for the performance of the Services. Use for the Supplier's own purposes, for work for other customers, for model training or for any other purpose is prohibited.

2.3 The Supplier follows the need-to-know principle and the principle of least privilege — it requests and uses only those access rights and permissions that are strictly necessary for the performance of the specific Service.

2.4 The Supplier complies with applicable law, the Client's contractual obligations towards its customers, the customer requirements communicated to the Supplier, and these Terms.

2.5 If the Supplier receives an instruction from the Client that conflicts with the security requirements of these Terms, with applicable law or with the security interests of the

Client or its customer, the Supplier must point out the conflict without delay and request confirmation or amendment of the instruction.

2.6 The Supplier acts so as to protect the good name and legitimate interests of the Client and its customers.

3. Accounts, Identities and Access Rights

3.1 The Supplier uses only accounts personally assigned to the specific individual who actually performs the Services.

3.2 Sharing accounts, passwords, tokens, certificates or other authentication means between multiple persons is prohibited.

3.3 The Supplier uses multi-factor authentication (MFA) wherever it is available or required by the Client.

3.4 The Supplier must not bypass, or attempt to bypass, security controls, authentication, authorisation, logging or communication filters.

3.5 The Supplier uses access rights only within the approved scope and for as long as it actually needs them for the performance of the Services. The Supplier notifies the Client without delay when an access right is no longer needed.

3.6 The Supplier notifies the Client without delay of any identified excessive, incorrectly assigned or unauthorised access to information or systems.

3.7 The Supplier acknowledges that the Client is entitled to immediately block an account, identity or access to an information system upon reasonable suspicion of a security incident or misuse of access, without prior notice; the Supplier will be informed of the blocking without undue delay.

3.8 The Supplier must not create, deploy or operate technical (service) accounts, shared accounts or automated integrations without the Client's prior approval.

4. Devices and Use of Private Devices (BYOD)

4.1 Unless otherwise agreed in a Partial Agreement, the Supplier provides the Services using its own devices. Every device used for the provision of the Services must meet the following security requirements:

a) a supported operating system with current security updates and up-to-date key applications;
b) system disk encryption where technically available;
c) active anti-malware protection approved by the Client;
d) an installed and active endpoint detection and response (EDR) tool approved by the Client;
e) automatic locking of the device after a set period of inactivity and locking of the screen when leaving the device;

f) strong authentication for access to the operating system (password, PIN, biometrics);

g) protection of the device against loss, theft and access by other persons, including family members.

4.2 The Supplier must not deactivate, uninstall, block or modify the security tools approved by the Client and operated on the device. The Supplier shall allow regular updates and maintenance of these tools and remote intervention as part of security incident response (in particular device isolation or removal of a malicious file).

4.3 The Supplier separates work data from private data to the extent corresponding to the technical capabilities of the device (e.g. a separate user profile, separate approved storage locations for work data, separate browsers or browser profiles).

4.4 The Supplier acknowledges and agrees that the security tools approved by the Client may, for security purposes, process technical data about the device (network communication including target destinations and ports, executed processes and their artefacts, file system changes without collecting the content of the Supplier's private documents, system logs, hardware configuration information) and detect malicious code. The Client does not use these tools to make audiovisual recordings, record the screen or log keystrokes.

4.5 The Supplier shall allow the Client to reasonably verify compliance with the requirements under Art. 4.1 in the manner set out in Art. 12 of these Terms. The Client has no right of blanket access to the Supplier's private data stored on the device.

4.6 In the event of loss or theft of, or unauthorised access to, a device used for the provision of the Services, the Supplier proceeds in accordance with Art. 9 of these Terms.

5. Information Handling

5.1 The Supplier respects the information classification determined by the Client or by the information owner on the side of the Client or its customer. All projects and engagements for the Client's customers are considered confidential unless a stricter designation is specified.

5.2 The Supplier stores the information of the Client and of the Client's customers only in storage locations and systems approved by the Client. Storing such information in private cloud storage, private e-mail, private media or unapproved communication services is prohibited.

5.3 For work communication, the Supplier uses only communication channels approved by the Client. For e-mail communication with work-related content, the Supplier uses only an approved e-mail client connected to the work identity.

5.4 Transfer of confidential information outside approved storage locations and channels requires the Client's approval and must be encrypted.

5.5 The Supplier does not disclose the information of the Client or of the Client's customers to unauthorised persons, including other personnel of the Supplier not involved in the given engagement.

5.6 The Supplier limits printing and the creation of local copies of information to the minimum necessary; printed materials must not be left unattended and must be securely shredded once no longer needed.

5.7 The Supplier must not use the information of the Client or of the Client's customers for another customer, for its own development or commercial products, for training or fine-tuning artificial intelligence models, or for any other own purposes.

5.8 Once no longer needed, the Supplier securely deletes local working copies of information; the procedure upon termination of cooperation is set out in Art. 13.

6. Software, Cloud Services and Licences

6.1 For the provision of the Services, the Supplier uses only software that is legally licensed for business / commercial use, receives security support from its vendor, and does not fall into the prohibited categories under the Client's current operational instruction.

6.2 The Supplier must not install or use software that:

a) is designed to bypass security measures (tunnelling tools, unapproved VPN clients, anonymisation networks);
b) enables remote access to the endpoint device outside the tools approved by the Client;
c) interferes with the security mechanisms of the device at kernel level or through security drivers, unless approved by the Client;
d) was obtained illegally, is cracked, modified through unofficial means, or comes from unofficial sources;
e) mines cryptocurrency;
f) is a web browser extension with access to login credentials, form content or sessions, unless approved by the Client.

6.3 The current list of prohibited or approved software categories and specific tools (including the approved anti-malware and EDR) is an operational instruction of the Client and is provided to the Supplier and updated in the manner set out in Art. 14.

6.4 The use of SaaS or cloud services for the performance of the Services requires the Client's prior approval. The approval is tied to the specific service, purpose and type of information processed.

6.5 The Supplier complies with the licence terms of proprietary and open-source software used in the performance of the Services. For open-source components with copyleft licences (in particular GPL and AGPL), the Supplier assesses the impact on the customer solution in advance and informs the Client.

6.6 The Supplier is responsible for all software, libraries, dependencies and extensions that it uses, installs or includes in a delivery in the performance of the Services.

7. Secure Development

7.1 This Article applies only to the extent that the Services include software development, source code management, testing, DevOps activities or the operation of applications of the Client or its customer.

7.2 Source code, configuration and related project documentation must be stored in a version-controlled repository approved by the Client. Storing production source code outside the approved repository (local archives, personal repositories, unapproved public services) is prohibited.

7.3 The Supplier does not store passwords, keys, tokens, certificates or other secrets directly in source code, in configuration files in the version-controlled repository, in logs or in publicly accessible locations. For their storage, the Supplier uses a secrets management tool approved by the Client.

7.4 The Supplier reviews the dependencies and libraries used from the perspective of licences and known vulnerabilities. Serious identified vulnerabilities are remediated with the priority and within the deadline set by the Partial Agreement or the customer's requirement.

7.5 The Supplier respects the code review and CI/CD controls configured for the given project. Bypassing branch policies, approval rules, automated tests or security checks is prohibited.

7.6 The Supplier does not introduce into source code any backdoors, hidden functions, telemetry sending data outside the approved environment, or other undocumented access paths or mechanisms.

7.7 The Supplier provides cooperation in security testing commissioned by the Client or its customer (in particular SAST, DAST, SCA and penetration tests) and in the verification of fixes.

7.8 The Supplier delivers a software bill of materials (SBOM) where required by the Partial Agreement or by the customer's security requirements for the specific delivery.

8. Use of Artificial Intelligence

8.1 The Supplier may use artificial intelligence tools for the performance of the Services only to the extent approved by the Client for the given project.

8.2 The Supplier must not enter into, or otherwise make available to, artificial intelligence tools not approved by the Client for the given purpose: internal information of the Client, information of the Client's customers, confidential and secret information, personal data, or source code outside approved cases.

8.3 The use of artificial intelligence must not infringe copyright, licence terms, personal data protection or the Client's contractual obligations towards its customer.

8.4 Outputs of artificial intelligence tools must be professionally reviewed by the Supplier before being used in a delivery. The Supplier is responsible for the output as if it had created it without the use of artificial intelligence.

8.5 The use of artificial intelligence must not bypass the security, quality, testing or approval processes established by the Agreement, the Partial Agreement or an operational instruction.

8.6 If the Supplier uses artificial intelligence in the development or processing of customer information and the nature of the activity so requires, the Supplier must transparently disclose this fact to the Client.

9. Security Incidents and Vulnerabilities

9.1 The Supplier must notify the Client of every security incident concerning the information or systems of the Client or its customers without undue delay, and in any case within 24 hours of detection or reasonable suspicion.

9.2 A security incident means, in particular: compromise or suspected compromise of a work account, malware infection, successful or likely successful phishing, loss or theft of a device used for the performance of the Services, leak or unauthorised disclosure of the Client's or a customer's information, accidental sharing of information with an unauthorised person, unauthorised access to information or systems, or loss of an authentication means (password, token, certificate).

9.3 The Supplier submits notifications under Art. 9.1 to security@greencode.cz or through another channel designated by the Client.

9.4 Until the Supplier receives the Client's instructions, the Supplier must:

a) preserve available logs, records and other evidence related to the incident;
b) refrain from irreversible steps (formatting, reinstallation, deletion) where the situation allows, unless immediate containment requires otherwise;
c) without undue delay, restrict the access of the compromised account or device to the Client's information.

9.5 The Supplier provides the Client with cooperation in containment, technical analysis, eradication, recovery and remediation, including the handover of relevant logs and artefacts.

9.6 The Supplier also notifies the Client of any identified serious vulnerability or misconfiguration in the information or systems of the Client or its customer to which the Supplier has access in the course of providing the Services.

10. Subcontractors and Other Persons

10.1 The involvement of other persons on the Supplier's side in the performance of the Services requires the Client's prior written consent in accordance with the Agreement.

10.2 The Supplier binds every such person to obligations to the extent of these Terms and is liable for their conduct as for its own.

10.3 The Supplier does not grant any such person broader access to the information and systems of the Client or its customer than is necessary for the performance of the part of the Services that the person provides.

11. Physical Security

11.1 When moving within the premises of the Client or its customer, the Supplier uses only personally assigned access means (access card, mobile application, identification means). Lending these means to other persons is prohibited.

11.2 The Supplier does not let into the Client's premises any persons whom it does not know or whose authorisation to enter it cannot verify. The Supplier escorts visitors only to the extent it is authorised to do so.

11.3 When leaving the workplace, the Supplier locks the workstation. Printed materials and media are stored so that they are not accessible to unauthorised persons.

11.4 The Supplier reports the loss of an access means, device or medium without delay in the manner set out in Art. 9.

11.5 On the premises of the Client's customer, the Supplier additionally follows the customer's security rules communicated to the Supplier.

12. Verification and Demonstration of Compliance

12.1 The Client is entitled to reasonably verify whether the Supplier complies with the obligations under these Terms and under the Client's operational instructions. The Client performs verification in particular through:

a) a security questionnaire or the Supplier's solemn declaration;
b) evidence of the device configuration (e.g. a screenshot or settings printout);
c) output from an approved security tool operated on the Supplier's device;
d) evidence of remediation of an identified deficiency;
e) a targeted inspection in the event of a security incident or reasonable suspicion thereof.

12.2 Verification under Art. 12.1 must be proportionate to the risk, limited to the scope relevant to the protection of the information and systems of the Client and its customers, and conducted in a manner that minimises access to the Supplier's private data.

12.3 The Supplier cooperates in audits performed by the Client's customer that are substantively related to a specific Partial Agreement, to the extent corresponding to the demonstration of compliance with security obligations; the costs of such cooperation are governed by the Agreement and the Partial Agreement.

13. Termination of Cooperation

13.1 As of the date of termination of the Agreement or a Partial Agreement, or earlier upon the Client's instruction, the Supplier:

a) ceases to use access to the information and systems of the Client and of the Client's customers;
b) returns devices, access cards, certificates, tokens and other means provided by the Client;
c) hands over to the Client work in progress, source code, documentation and other outputs in the state corresponding to the latest agreement;
d) removes local and other copies of the information of the Client and of the Client's customers stored on the Supplier's devices, unless their retention is required by law.

13.2 Upon the Client's request, the Supplier confirms in writing that it has fulfilled the obligations under Art. 13.1.

13.3 The duty of confidentiality and information protection under the Agreement survives the termination of cooperation.

14. Operational Instructions and Exceptions

14.1 The Client may provide the Supplier with current operational security instructions, in particular the list of prohibited or approved software categories, the list of approved security tools, classification rules, contact channels and specific customer requirements. An operational instruction cannot extend the Supplier's contractual obligations, financial costs or scope of liability beyond these Terms and the Partial Agreement.

14.2 An exception from a specific requirement of these Terms must be approved in advance and in writing by the Client's Security Manager. An exception may be time-limited and subject to compensating measures.

14.3 In the event of an imminent security risk, the Client is entitled to temporarily restrict or block the Supplier's access to information or systems. The Client informs the Supplier of the reason and expected scope without undue delay.

14.4 The Supplier remedies any identified non-compliance without undue delay after the Client's request; in the case of a serious deficiency, the Supplier takes immediate measures to mitigate the risk even before full remediation.

15. Changes to the Terms

15.1 The Client is entitled to unilaterally amend these Terms to a reasonable extent in accordance with the Agreement, in particular due to the evolution of security threats, changes in legal requirements or the requirements of the Client's customers.

15.2 An amendment to the Terms is notified to the Supplier at least 30 days before it takes effect, in the manner set out in the Agreement. Unless the Supplier terminates the Agreement in accordance with the Agreement, the amendment takes effect on the date

stated therein. If the Supplier terminates the Agreement due to disagreement with the amendment, the relationship of the parties remains governed by the existing wording of the Terms until the expiry of the notice period.

15.3 The current and archived versions of the Terms are published at https://www.greencode.cz/legal/terms. Each version includes a version number and effective date.

16. Final Provisions

16.1 The consequences of a breach of these Terms are governed by the Agreement. These Terms do not introduce any separate contractual penalties.

16.2 In case of any discrepancy between the Czech wording and any language translations of these Terms, the Czech wording prevails.

Version history:

Version	Effective from	Description
1.0	[TO BE COMPLETED]	Initial release