Gurobi Security Addendum

This Security Addendum ("**Addendum**") is a Published Policy that describes the security measures Gurobi maintains for hosted Product deployments. This Addendum is incorporated into the Gurobi Master License Agreement ("**MLA**") and, to the extent applicable, the Gurobi Online Terms of Service ("**Online Terms**"). The MLA or the Online Terms, as applicable, is the "**Agreement**." Capitalized terms not defined in this Addendum have the meanings given in the Agreement, the Product Licensing Policy, or the Cloud Supplement. If this Addendum conflicts with the Agreement, the Agreement controls. Each Order Form is governed by the version of this Addendum in effect on the date of that Order Form, as provided in the MLA.

1. Scope. This Addendum applies to (i) Instant Cloud and (ii) Gurobi's storage and handling of Model Input Files and other information that Customer provides to Gurobi under the Agreement (collectively, the "Covered Systems"). This Addendum does not apply to the Web License Service, which is license administration infrastructure that does not host, process, or store Customer's optimization models, Model Input Files, or other Customer data. This Addendum does not apply to Customer's installation or operation of the Product on infrastructure Customer controls under an On-Prem License, which is Customer's responsibility as described in the On-Prem Supplement.

2. Definitions.
2.1 "Customer Data" has the meaning given in the Cloud Supplement and includes Model Input Files that Customer provides to Gurobi.
2.2 "Security Incident" means a confirmed breach of security of the Covered Systems leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data. Unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, and denial-of-service attacks, are not Security Incidents.

3. Security Program. Gurobi will maintain a written information security program with administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Customer Data in the Covered Systems, appropriate to the nature of the Covered Systems and the risks presented. Gurobi will review its security program at least annually. Gurobi will provide information about its security controls under Section 12 on request.

4. Personnel. Gurobi will (i) require personnel with access to Customer Data to be bound by confidentiality obligations, (ii) conduct background checks on such personnel where permitted by applicable law, and (iii) provide security awareness training to such personnel.

5. Access Control. Gurobi will (i) limit access to Customer Data to personnel who need access to perform under the Agreement, (ii) use unique user accounts and multi-factor authentication for administrative access to the Covered Systems, and (iii) promptly revoke access when it is no longer required.

6. Encryption. Gurobi will encrypt Customer Data in transit over public networks to and from the Covered Systems using TLS 1.2 or higher. Gurobi will encrypt at rest the Instant Cloud management database.

7. Infrastructure. Instant Cloud runs on Cloud Provider infrastructure. Physical and environmental security of that infrastructure is provided by the Cloud Provider. Gurobi is responsible for the security of the Instant Cloud environment it configures and manages on that infrastructure.

8. Vulnerability Management and Monitoring. Gurobi will (i) maintain processes to identify, assess, and remediate vulnerabilities in the Covered Systems in a timely manner based on risk, (ii) apply security patches to the Covered Systems in a timely manner, and (iii) maintain logging and monitoring of the Covered Systems designed to detect unauthorized access.

9. Business Continuity. Gurobi will maintain measures designed to restore the availability of the Covered Systems after a disruption. Instant Cloud is not a data storage or backup service, and Customer remains responsible for backups of Customer Data as provided in the Cloud Supplement. Availability commitments and Service Level Credits for Instant Cloud and the Web License Service are set forth exclusively in the Cloud Supplement and the On-Prem Supplement, respectively.

10. Security Incidents.

10.1 Notice. Gurobi will notify Customer of a Security Incident without undue delay, and in any event within seventy-two (72) hours, after Gurobi confirms the Security Incident. Gurobi will send notice to the Customer Notice Contact on the applicable Order Form or, if none, to the email address associated with Customer's account.

10.2 Content. Gurobi's notice will describe, to the extent then known, the nature of the Security Incident, the categories of Customer Data affected, and the measures Gurobi has taken or proposes to take. Gurobi will supplement its notice as more information becomes available.

10.3 Cooperation. Gurobi will take reasonable steps to contain and remediate the Security Incident and will provide reasonable cooperation to Customer in connection with Customer's own notification obligations.

10.4 No Admission. Gurobi's notice of or response to a Security Incident is not an acknowledgment of fault or liability.

10.5 License Credentials. Customer's obligation to notify Gurobi of any compromise of License Credentials is governed by the EULA.

11. Customer Responsibilities. Customer is responsible for (i) securely configuring its use of the Covered Systems, (ii) protecting its License Credentials, (iii) managing Authorized User access, (iv) encrypting Customer Data as appropriate before submitting it, (v) maintaining backups of Customer Data, and (vi) securing its own systems, networks, and infrastructure, including all infrastructure used under an On-Prem License. Customer will not include personal data in Model Input Files unless necessary for Customer's use of the Product, as provided in the Data Processing Addendum.

12. Assessments. Upon Customer's written request, no more than once in any twelve (12) month period, Gurobi will provide a written summary of its security controls or complete a reasonable security questionnaire. Information Gurobi provides under this Section is Gurobi's Confidential Information. Customer may not perform penetration testing, vulnerability scanning, or other security testing of the Covered Systems without Gurobi's prior written consent.

13. Subprocessors. Gurobi's use of subprocessors that process personal data is governed by the Data Processing Addendum.

14. Deletion. Deletion of Customer Data in Instant Cloud after expiration or termination is governed by the Cloud Supplement. Deletion of Model Input Files from the Gurobi model library is governed by the Agreement.

15. Changes. Gurobi may update this Addendum from time to time. Updates will not materially reduce the overall level of protection provided for Customer Data during the then-current term of an existing Order Form.

16. Liability. Each party's liability arising out of or relating to this Addendum is subject to the general limitations of liability in the Agreement. A breach of this Addendum is not a breach of the confidentiality provisions of the Agreement for purposes of any increased liability cap that applies to breaches of confidentiality.