## Schedule 1 – Information Security

1. **Standards Compliance**. Revenera has and will maintain SOC2 certification throughout the subscription term of the Order and will and make reports on the same available to the Customer upon request.

2. **Security Organization.** Revenera has and will maintain an information security function, which has responsibility for ensuring good practice in relation to information security and in relation to the provision of the SaaS and Services, including the publication of information security policies.

3. **Reporting and Incident Management.**

   a. Revenera has implemented procedures for Information Security Incidents to be reported through appropriate management channels as quickly as reasonably possible. All employees and representatives of Revenera or their sub-contractors will be made aware of their responsibility to report Information Security Incidents as quickly as reasonably possible.
   b. Revenera has and will maintain procedures to ensure a quick, effective, and orderly response to Information Security Incidents.
   c. Revenera has and will maintain an incident classification scale in place to decide whether a security event should be classified as an Information Security Incident. The classification scale will be based on the impact and extent of an incident.
   d. Revenera will without undue delay (within 48 hours from confirmation) notify Customer of any Information Security Incidents. Notifications to Customer will be sent to an address to be provided by Customer.
   e. If an Information Security Incident reveals any deficiencies, weaknesses, or areas of non-compliance, Revenera will promptly take such steps as may be required, in Revenera's reasonable discretion, to address material deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable given the circumstances.
   f. Upon request, Revenera will keep Customer informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same, and will certify to Customer as soon as may be practicable given the circumstances that all necessary remedial actions have been completed.
   g. For the purposes of this Section, "Information Security Incidents" will mean any unmitigated security incident, of which Revenera has actual knowledge and which (i) compromises or is likely to compromise the security or integrity of Customer data or systems, or (ii) otherwise materially affects Revenera's ability to comply with the obligations in this Schedule.

4. **Security Testing.** Revenera has arranged for all testing as detailed in this Section below to be undertaken by an independent third party.

   a. Revenera, through its contractors, will perform penetration testing on the Revenera's systems no more than once every twelve (12) months. If the penetration testing conducted discovers vulnerabilities in Revenera's systems, Revenera will, to the extent that such vulnerabilities result in an inability to materially comply with this Schedule, remediate such vulnerabilities and re-perform the penetration testing focusing on those vulnerabilities discovered from the initial penetration testing. Upon receipt of a written request, Revenera will make available the penetration testing executive summary report to Customer.
   b. Revenera will, upon request, provide mutually agreed metrics at an agreed frequency to Customer to illustrate the performance of the testing schedule.

5. **Security Communication and Assistance.**

   a. Except as required by mandatory applicable law or by existing applicable contractual obligations, Revenera agrees that it will not inform any third party of any Information Security Incident referencing, or identifying the Customer, without Customer's prior written consent. Revenera will fully cooperate with Customer and law enforcement authorities concerning any unauthorized access to Customer's systems or networks, or data. Such co-operation will include the retention of all information and data within Revenera's possession, custody, or control that is directly related to any Information Security Incident.
   b. If disclosure is required by law, Revenera will work with Customer regarding the timing, content, and recipients of such disclosure.
   c. Revenera will respond promptly to any reasonable Customer requests for information, cooperation, and assistance, including to a Customer designated response center.

6. **Access Management.**

   a. Where Revenera personnel are accessing Customer systems or data, Revenera is responsible for validating the identity of such personnel.
   b. Revenera will ensure that when accessing Customer systems or data, Revenera personnel have the minimal required system access to carry out their duties and will not use shared accounts or password.
   c. Revenera will ensure that access to the Customer systems or data is governed by this Schedule.

7. **Security Review.** Subject to the conditions set out herein, Revenera will permit Customer personnel or authorized representatives to review and assess Revenera's compliance with the obligations set out in this Section ("**Security Review**"). The definition of audit rights is to be mutually agreed between Revenera and Customer. Unless otherwise required by law:
   a. Any Security Review is subject to not less than 28 days advance written notice and limited to no more than once in any 12-month period;

b. The Security Review will take place during normal business hours and should be conducted in a manner to minimize disruption to Revenera's business operations;
c. Customer will bear its own costs in relation to a Security Review; and
d. Any third party undertaking the Security Review must (i) be subject to confidentiality obligations no less protective than those set out in the Agreement; and (ii) must not be a competitor of Revenera.

8. **Business Continuity Management.** Revenera has and will maintain a documented Business Continuity and Disaster Recovery Plan ("**BC DR Plan**") throughout the term of the Agreement which will be tested, the results of which will be shared with the Customer upon request. Revenera has and will maintain emergency and contingency plans for the facilities that process Customer data.