Service Level Agreement

Product Service Level Description

"Severity 1" means “System Down” or a product-inoperative condition impacting a production environment for which no Workaround is immediately available, such as

(i) production server or other mission critical systems are down;

(ii) a substantial portion of mission-critical data is at a significant risk of loss or corruption;

(iii) a substantial loss of service;

(iv) business operations have been severely disrupted; or

(v) an incident with the erwin, Inc. software, catastrophic network or system failure or that compromises overall system integrity or data integrity when the software is installed or when it is in operation (i.e. system crash, loss or corruption of data, or loss of system security) and significantly impacts ongoing operations in a production environment.

SEVERITY 1 INCIDENTS MUST BE SUBMITTED TO ERWIN VIA TELEPHONE. IN ADDITION, THE ELEVATION OF ANY LOWER SEVERITY INCIDENT TO SEVERITY 1 STATUS MUST BE REQUESTED VIA TELEPHONE.

"Severity 2" means a high-impact business condition possibly endangering a production environment. The software may operate but is severely restricted.

"Severity 3" means a low-impact business condition with majority of software functions still usable; however, some circumvention may be required to provide service.

"Severity 4" means:

(i) a minor problem or question that does not affect the software function,

(ii) an error in software product Documentation that has no significant effect on operations; or

(iii) a suggestion for new features or software product enhancement. Service Level Objectives

Incident Severity Initial Response Time

Severity Level 1 1 hour

Severity Level 2 2 business hours

Severity Level 3 4 business hours

Severity Level 4 1 business day

Technical support availability & global opening times:

Severity 2 through 4 (24 x 5)

Severity 1 is for Production System Down (24 x 7)

Monday to Friday (excluding local public and bank holidays):

8:30 to 18:00 EST (All Americas)

8:30 to 17:30 GMT (EMEA & ROW*)

9:30 to 18:00 IST (EMEA region & ROW*)

6:00 to 15:00 SST (EMEA & ROW*)

Rest Of the World*

Remote diagnostics consist of screen sharing sessions to enable erwin, Inc. engineers to be fully understand the Service Incident problem. No other remote access to LICENSEE Systems is authorized under this Agreement and any request for remote access shall be approved in writing by LICENSEE and always supervised by LICENSEE.

Other diagnostics include but are not limited to:

product generated logs.

product error messages.

erwin Support may create utilities for specific problems (such as checking port availability).

Additionally, erwin provides industry standard diagnostics such as SQL Trace logs, Ipconfig, etc., which are typically installed with common operating systems and DBMS), or custom scripts.

erwin, Inc. will explain all diagnostic methods prior to implementation to allow LICENSEE to fully evaluate any possible impact on their systems.

One-off patches may be created to correct a specific erwin, Inc. Application Software defect.

Methods and the degree of testing code changes will vary depending on the nature and extent of the code changes.

Patches may be periodically included in a Maintenance Release posted to the erwin, Inc. support Web Site. Maintenance Releases typically receive automated QA and manual testing for specific maintenance coding.

Service Packs may include other Maintenance Releases as well as occasional design changes when necessary to address customer concerns, and typically are GA quality with full automated testing and manual testing.

New Version typically contain the maintenance changes above, and new features. These also are posted on the erwin, Inc. web site.

Cloud Hosting Service Levels

1) Access. erwin, Inc. shall make the Service available twenty-four (24) hours per day, seven (7) days a week with a minimum uptime level of ninety-nine and nine tenths of a percent (99.9%) measured on an aggregate monthly basis. Such service availability does not, however, include regularly scheduled maintenance or any unscheduled downtime due to failures beyond erwin, Inc.'s control (such as errors or malfunctions due to Customer's computer systems, local networks or Internet connectivity).
2) Scheduled Maintenance and Upgrades. erwin, Inc. shall conduct scheduled service maintenance of the Service ("Scheduled Maintenance") after normal business hours or on weekends, where possible. If this is not possible, erwin support staff will work with the customer admin to minimise disruption during peak working times. erwin, Inc. shall give the

Customer at least forty-eight (48) hours prior notice of the exact date and time of such Scheduled Maintenance via e-mail or other timely means of communication.

a) Upgrades can be requested by a customer admin contact 30 days after the release of a new version of an erwin application. The Hosting contract entitles the customer to one major version upgrade per year within the hosting price. Downtime will need to be scheduled with the customer admin contact for upgrade requests. Downtime will be minimized, as upgrade employees will be trained and practised in the upgrade of the software and if scheduled can be outside of peak environment usage times.

3) **Data Retention and Recovery**. erwin, Inc. shall backup the Service as follows: (a) daily full server backups, kept for 14 days (b) weekly full server backups, kept for 2 months, offering up to 60 days of backup. Backups will be stored in encrypted form, either in a secure secondary data centre location or using a Cloud Service Provider service, that offers redundancy as standard. erwin, Inc. shall implement sufficient measures to ensure that the backup data is accessible and maintained in a manner to enable restoration of the backup version of the Service in the event of a system malfunction or outage.
   a) erwin will ensure that Recovery Point Objective and Recovery Time Objective of environments are 24 hours, where possible. A disaster recovery test will be performed annually, to ensure the processes used, resources needed, and data format are correct, to allow this timeframe to be achieved.
   b) erwin will restore the service to a mutually agreed backup point, as part of normal service delivery, if an issue in data integrity is seen, as the result of issues with the service being delivered i.e. issues with maintenance activities, the infrastructure, services or the application itself. erwin does not guarantee to restore the data to a backup point, due to a customer end user having corrupted data or having incorrectly removed data from the system, whilst using the application or its API's. The customer should reach out to the erwin service desk and an assessment will be made on what can be done. This may incur additional cost.
4) **Requests for Support.** erwin, Inc. service representatives will be available to respond to support requests via email, online ticketing portal and phone during our support hours-See Product Service Level Description and online Self-Service Portal for details.
5) **Support Response Time.** erwin, Inc. support representatives shall respond to all customer support requests in a timely and professional manner and in accordance with our Product Service Level Description attached.
6) **Security Measures.** erwin, Inc. shall take, at a minimum, the following measures to protect the Service:
   - Single tenancy, with dedicated Virtual Private Cloud
   - Encryption in transit (TLS 1.2 and security certificates)
   - Encryption at rest (DB encryption, as part of RDBMS licensing) – This may incur additional cost
   - Firewall and security groups
   - IP whitelisting available at customer request
   - Anti-virus
   - Role-based access control

- Multi-factor authentication (used at both an environment administration level and via SAML2 at application level)
- Full segregation of hosting environments from any standard erwin internal network, ensuring segregation of duties and no service data transfer.
- Vulnerability scanning and Penetration testing (performed annually as part of the service) – performing more frequently may incur additional cost
- Intrusion detection/prevention – This will incur additional cost
- SIEM for event/log investigation, triage and log protection, above the standard log retention - This will incur additional cost.

SaaS Service Levels

1) Access. erwin, Inc. shall make the Service available twenty-four (24) hours per day, seven (7) days a week with a minimum uptime level of ninety-nine and nine tenths of a percent (99.9%) measured on an aggregate monthly basis. Such service availability does not, however, include regularly scheduled maintenance or any unscheduled downtime due to failures beyond erwin, Inc.'s control (such as errors or malfunctions due to Customer's computer systems, local networks or Internet connectivity).

2) Scheduled Maintenance and Upgrades. erwin, Inc. shall conduct scheduled service maintenance of the Service ("Scheduled Maintenance") after normal business hours or on weekends, where possible. If this is not possible, erwin support staff will work with the customer admin to minimise disruption during peak working times. erwin, Inc. shall give the Customer at least forty-eight (48) hours prior notice of the exact date and time of such Scheduled Maintenance via e-mail or other timely means of communication.
    a) Upgrades are automatically delivered to all systems at the same time, so downtime will be limited for product updates. Customers must receive the product updates at the same time as the other environments.
3) **Data Retention and Recovery**. erwin, Inc. shall backup the Service as follows: (a) daily full server backups, kept for 14 days (b) weekly full server backups, kept for 2 months, offering up to 60 days of backup. Backups will be stored in encrypted form, either in a secure secondary data centre location or using a Cloud Service Provider service, that offers redundancy as standard. erwin, Inc. shall implement sufficient measures to ensure that the backup data is accessible and maintained in a manner to enable restoration of the backup version of the Service in the event of a system malfunction or outage.
    a) erwin will ensure that Recovery Point Objective and Recovery Time Objective of environments are 24 hours, where possible. Customer specific security or configuration needs may push times beyond this (single tenant environments only) and this will be agreed with the customer. A disaster recovery test will be performed annually, to ensure the processes used, resources needed and data format are correct, to allow this timeframe to be achieved.

b) erwin will restore the service to a mutually agreed backup point, as part of normal service delivery, if an issue in data integrity is seen, as the result of issues with the service being delivered i.e. issues with maintenance activities, the infrastructure, services or the application itself. erwin does not guarantee to restore the data to a backup point, due to a customer end user having corrupted data or having incorrectly removed data from the system, whilst using the application or its API's. The customer should reach out to the erwin service desk and an assessment will be made on what can be done. This may incur additional cost.

4) **Requests for Support.** erwin, Inc. service representatives will be available to respond to support requests via email, online ticketing portal and phone during our support hours-See Product Service Level Description and online Self-Service Portal for details**.**

5) **Support Response Time.** erwin, Inc. support representatives shall respond to all Customer support requests in a timely and professional manner and in accordance with our Product Service Level Description. **Security Measures.** erwin, Inc. shall take, at a minimum, the following measures to protect the Service:

- Multi tenancy offering with shared VPC and also Single tenancy offering, with dedicated VPC
- Encryption in transit (TLS 1.2 and security certificates)
- Encryption at rest (DB encryption, as part of DB as a service)
- Firewall and security groups
- Resource monitoring and resource threshold alerting
- IP whitelisting available at customer request (Single tenant only)
- Anti-virus
- Role-based access control
- Multi-factor authentication (used at both an environment administration level and via SAML2 at application level)
- Full segregation of SaaS environments from any standard erwin internal network, ensuring segregation of duties and no service data transfer.
- Vulnerability scanning and Penetration testing (performed annually as part of the service) – performing more frequently may incur additional cost
- Intrusion detection/prevention – This will incur additional cost
- SIEM for event/log investigation, triage and log protection, above the standard log retention - This will incur additional cost.