

Specimen — illustrative example

Solstice Grid Services is a fictional organisation. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

Third-Party AI Review Procedure

Solstice Grid Services

Document type	procedure	Version	1.0 Draft
Owner	Head of Engineering	Customer decision role	Chief Technology Officer
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Ontario, Canada		
Prepared for	Solstice Grid Services	Industry	Energy and utilities
Organization size	101-500	Locations	Not specified

Advisory draft for accountable-owner and professional review. Validate legal, regulatory, contractual, technical and operational requirements before customer release. This is not legal advice, a certification, or a compliance determination.

1. Purpose

This procedure establishes the ordered steps Solstice Grid Services follows to evaluate, review and monitor AI-enabled suppliers before and during their engagement. It ensures that third-

party AI systems meet the organisation's requirements for security, privacy, model governance, human oversight and contractual protection before any data is shared or any capability is granted.

2. Scope

This procedure applies to any supplier whose product or service incorporates artificial intelligence, machine learning or autonomous decision-making capability and that will:

- a) Receive, process or store Solstice Grid Services data, including grid telemetry, consumption data linked to service addresses, or outbound correspondence content.
- b) Make or inform decisions affecting grid operations, customer service, billing or workforce scheduling.
- c) Act autonomously or semi-autonomously within Solstice Grid Services systems.

The procedure covers the full supplier lifecycle: initial due diligence, contract formation, ongoing monitoring and exit.

3. Definitions

AI provider: A supplier whose product or service uses artificial intelligence, machine learning or autonomous decision-making to process Solstice Grid Services data or to take or recommend actions on the organisation's behalf.

Training use: Any use of Solstice Grid Services data to train, fine-tune, reinforce or otherwise improve a machine-learning model, whether the provider's own model or a third party's.

Subprocessor: Any entity other than the AI provider that processes Solstice Grid Services data on the provider's behalf, including hosting providers, model vendors and analytics services.

Model change: Any update to the AI provider's model weights, architecture, training data, inference logic or action capability that could alter the outputs or behaviours Solstice Grid Services relies on.

Exit capability: The provider's demonstrated ability to return or securely delete all Solstice Grid Services data, disable any action capability and terminate processing within a defined period when the engagement ends.

4. Roles and Responsibilities

Requesting Business Owner: The manager or lead who identifies the need for the AI-enabled supplier. Responsible for documenting the use case, data flows and business criticality, and for sponsoring the engagement through review.

Head of Engineering (Document Owner): Owns this procedure. Conducts or coordinates the technical and security assessment. Maintains the AI supplier register. Escalates findings that exceed defined thresholds.

Privacy Officer: Assesses privacy implications, confirms data residency and training-use commitments, and validates that contract terms meet applicable Ontario privacy requirements.

Chief Technology Officer (Decision Role): Holds review authority for Critical-tier AI suppliers and for any engagement that grants action capability. Accepts or rejects residual risk. Authorises exceptions.

Control Room Supervisor: Consulted when the AI provider's outputs or actions could affect operational technology or grid reliability. Confirms that action boundaries exclude operational technology.

Legal or Procurement Lead: Ensures contract terms reflect the requirements identified during review and that exit provisions are enforceable.

5. Supplier Risk Tiering

Before detailed review begins, the Requesting Business Owner assigns a risk tier using the criteria below.

5.1 Critical Tier

Assign Critical when any of the following is true:

- a) The supplier is the agent orchestration platform, the model provider, the telemetry pipeline vendor or the mapping data provider.
- b) The supplier will receive consumption data linked to service addresses.
- c) The supplier's system will take autonomous actions within Solstice Grid Services environments.

d) Failure or compromise of the supplier would materially impair grid operations, billing or customer service.

Critical-tier engagements require Chief Technology Officer review before any data is shared or action capability is granted.

5.2 Standard Tier

Assign Standard when the supplier meets the scope criteria in Section 2 but none of the Critical criteria above. Standard-tier engagements require Head of Engineering review.

5.3 Tier Escalation

If review findings reveal risks not apparent at initial tiering, the reviewer escalates the tier and restarts review at the higher level.

6. Procedure Steps

The steps below are performed in sequence. Each step names the responsible role, the required inputs, the actions and the outputs recorded.

6.1 Step 1: Initiate Request

Role: Requesting Business Owner

Inputs: Business need, candidate supplier, preliminary data and integration scope.

Actions:

1.1 Complete the AI Supplier Intake Form, documenting:

- The use case and business problem the supplier addresses.
- The data categories the supplier will receive (grid telemetry, consumption data, correspondence content, other).
- The decisions or actions the supplier's system will make or inform.
- The integration points with Solstice Grid Services systems.
- The business criticality: impact if the supplier fails or is compromised.

1.2 Assign the initial risk tier per Section 5.

1.3 Submit the form to the Head of Engineering.

Outputs: Completed AI Supplier Intake Form with assigned tier, recorded in the AI supplier register.

6.2 Step 2: Security and Technical Assessment

Role: Head of Engineering

Inputs: AI Supplier Intake Form, supplier security documentation, penetration test reports, certifications.

Actions:

2.1 Request from the supplier:

- Current security certifications and audit reports.
- Architecture documentation showing data flows, encryption in transit and at rest, and access controls.
- Penetration test or vulnerability assessment results from the prior twelve months.
- Incident history and notification track record.

2.2 Assess against the requirements in the Information Security Policy and the Data Classification and Handling Standard.

2.3 Confirm that the supplier's infrastructure keeps Solstice Grid Services data within Canada.

2.4 Identify gaps and record them with severity (Critical, High, Medium, Low).

Outputs: Security Assessment Record listing findings, gaps and severity ratings.

6.3 Step 3: Privacy and Data Governance Assessment

Role: Privacy Officer

Inputs: AI Supplier Intake Form, supplier privacy documentation, data processing agreement drafts.

Actions:

3.1 Confirm whether the supplier will process personal information (consumption data linked to service addresses is personal information).

3.2 Verify the supplier's commitment that no Solstice Grid Services data will be used for training, fine-tuning or model improvement.

3.3 Verify data residency: all personal information must remain in Canada.

3.4 Identify all subprocessors and confirm each meets the same data residency and training-use restrictions.

3.5 Confirm retention periods and deletion commitments align with the Records Retention and Disposal Policy.

3.6 Record gaps and required contract terms.

Outputs: Privacy Assessment Record listing findings, required contract clauses and residual privacy risk.

6.4 Step 4: Model Governance and Transparency Assessment

Role: Head of Engineering, with Privacy Officer input

Inputs: Supplier model documentation, change-notification commitments, explainability materials.

Actions:

4.1 Document the model's purpose, the inputs it consumes and the outputs or actions it produces.

4.2 Assess output quality: request accuracy, error rate or performance metrics relevant to the use case.

4.3 Confirm the supplier's change-notification commitment: Solstice Grid Services must be notified before any model change that could alter outputs or behaviours.

4.4 Assess transparency: can Solstice Grid Services explain to affected parties (customers, regulators, employees) how the system reaches its outputs?

4.5 For suppliers whose systems take autonomous actions, confirm:

- Action logging with inputs, outputs and timestamps.
- Logs are retained and exportable.
- Solstice Grid Services can revoke action capability immediately without terminating the contract.

4.6 Record gaps.

Outputs: Model Governance Assessment Record.

6.5 Step 5: Human Oversight and Action Boundary Verification

Role: Head of Engineering, with Control Room Supervisor consultation for grid-affecting systems

Inputs: AI Supplier Intake Form, supplier technical documentation, action boundary definitions.

Actions:

5.1 Confirm the human oversight model:

- For autonomous agents: daily engineer review of action logs; any action outside the defined boundary halts the agent until a human clears it.
- For correspondence drafting: human review before sending.

5.2 For any supplier whose outputs or actions could affect grid operations, confirm with the Control Room Supervisor that the action boundary excludes:

- Load switching.
- Protection settings.
- Any action on the operational technology network.

5.3 Confirm reversibility: actions taken by the agent must be reversible.

5.4 Record any gaps in oversight or boundary enforcement.

Outputs: Human Oversight Verification Record.

6.6 Step 6: Consolidate Findings and Determine Contract Requirements

Role: Head of Engineering

Inputs: All assessment records from Steps 2–5.

Actions:

6.1 Consolidate findings into a single AI Supplier Review Summary.

6.2 List required contract terms, including at minimum:

- Notification before any model or agent capability change.
- No training on customer or telemetry data.
- Action logging retained and exportable.
- Incident notification within a period set by Solstice Grid Services and recorded in the contract; 24 hours is the organisation's current position and is not derived from a cited control.
- Subprocessor additions require Solstice Grid Services written consent.
- Right to revoke action capability immediately without terminating the contract.
- Data return or certified deletion at exit within a period set by Solstice Grid Services and

recorded in the contract; 30 days is offered as a starting point.

- Data residency in Canada.

6.3 Identify any gaps the supplier cannot or will not close.

6.4 State the residual risk if the engagement proceeds with those gaps.

Outputs: AI Supplier Review Summary with required contract terms, unresolved gaps and residual risk statement.

6.7 Step 7: Review Decision

Role: Chief Technology Officer (Critical tier) or Head of Engineering (Standard tier)

Inputs: AI Supplier Review Summary.

Actions:

7.1 Review the summary, required contract terms and residual risk.

7.2 Decide one of:

- Proceed: All requirements met or gaps closed. Engagement may proceed once contract is executed.
- Proceed with conditions: Gaps remain but residual risk is accepted. Document the accepted risk, the compensating controls and the review date.
- Reject: Residual risk exceeds tolerance. Engagement does not proceed.

7.3 For Critical-tier suppliers or any supplier granted action capability, the Chief Technology Officer records the decision. For Standard-tier suppliers without action capability, the Head of Engineering records the decision.

7.4 If an exception to this procedure or to a required contract term is requested, the Chief Technology Officer must review and accept it, with an expiry date no longer than twelve months.

Outputs: Review Decision Record with decision, conditions, accepted residual risk and any exception with expiry date.

6.8 Step 8: Contract Execution

Role: Legal or Procurement Lead, with Head of Engineering and Privacy Officer confirmation

Inputs: Review Decision Record, required contract terms.

Actions:

8.1 Ensure the contract incorporates all required terms from the Review Summary.

8.2 Head of Engineering and Privacy Officer confirm the executed contract reflects the requirements.

8.3 Record the contract execution date and term in the AI supplier register.

Outputs: Executed contract; updated AI supplier register entry.

6.9 Step 9: Ongoing Monitoring

Role: Head of Engineering

Inputs: Supplier notifications, incident reports, action logs, contract terms.

Actions:

9.1 Monitor for material changes:

- Model changes notified by the supplier.
- Subprocessor changes.
- Security incidents or breaches.
- Changes to data residency or training-use commitments.

9.2 Review supplier-provided action logs on a schedule set by Solstice Grid Services; daily review is the current position for autonomous agents.

9.3 If the supplier notifies a material change, assess whether it alters the risk profile. If it does, return to Step 2 and repeat the relevant assessments.

9.4 If the supplier fails to notify a change that should have been notified, record the failure and escalate to the Chief Technology Officer.

9.5 Conduct a full re-review at least annually, or more frequently if the Review Decision Record specifies.

Outputs: Monitoring log entries; re-review records as required.

6.10 Step 10: Exit and Data Return or Deletion

Role: Head of Engineering, with Privacy Officer confirmation

Inputs: Decision to terminate engagement, contract exit provisions.

Actions:

10.1 Notify the supplier of termination per contract terms.

10.2 Revoke any action capability immediately.

10.3 Request data return or certified deletion within the period specified in the contract.

10.4 Obtain written certification from the supplier that all Solstice Grid Services data has been returned or securely deleted, including from subprocessors.

10.5 Privacy Officer confirms the certification is complete.

10.6 Update the AI supplier register to reflect terminated status and retain the exit records per the Records Retention and Disposal Policy.

Outputs: Data return or deletion certification; updated AI supplier register; exit record retained.

7. Records and Register

The Head of Engineering maintains the AI supplier register, which records for each AI provider:

- a) Supplier name and description of AI capability.
- b) Risk tier.
- c) Dates of intake, assessment completion and review decision.
- d) Review decision and any conditions or accepted residual risk.
- e) Contract execution date and term.
- f) Exception details and expiry dates, if any.
- g) Monitoring events: material changes, incidents, re-reviews.
- h) Exit date and data return or deletion certification, if terminated.

Assessment records, review decisions and exit certifications are retained per the Records Retention and Disposal Policy.

8. Metrics

The Head of Engineering reports the following metrics to the Chief Technology Officer on a schedule set by Solstice Grid Services; quarterly is offered as a starting point:

- a) AI suppliers reviewed before use: count of suppliers that completed this procedure before any data was shared or action capability granted, as a percentage of all new AI supplier engagements.
- b) Contract gaps with treatment recorded: count of engagements where gaps were identified and a documented treatment (remediation, compensating control or accepted risk) was recorded.
- c) Percentage of required reviews completed on time: annual re-reviews and condition-driven reviews completed by their due date.
- d) Number of exceptions past their expiry date: exceptions that have not been renewed or closed.

e) Number of material control failures and overdue corrective actions: incidents where a supplier failed a contractual control and corrective actions remain open past their target date.

9. Related Documents

This procedure operates under and alongside:

- AI Governance and Accountability Policy
- Third-Party Risk Management Policy
- Information Security Policy
- Privacy and Personal Information Policy
- AI Risk Management Standard
- Data Classification and Handling Standard
- Records Retention and Disposal Policy
- AI Incident Response Procedure
- Security Incident Response Procedure
- Privacy Breach Response Procedure

10. Document Control

Document Owner: Head of Engineering

Review Authority: Chief Technology Officer

Review Frequency: Annual, or following a material change to AI supplier risk, regulatory requirements or organisational structure.

Version: 1.0

Effective Date: Upon review by the Chief Technology Officer.

Owner review items

The drafting process identified the following in the supplied answers. Resolve each before customer release.

Type	Detail	Where
gap	No verified framework controls were supplied. This procedure is based on RiskWoven AI practical best practices as stated in the specification, but no specific control identifiers or citations are available to reference.	Entire document
gap	The organisation's existing Third-Party Risk Management Policy, AI Risk Management Standard and other referenced documents were identified by title and type only. This procedure assumes alignment but cannot verify specific requirements or thresholds those documents contain. The organisation must reconcile this procedure with the actual content of those documents.	Section 9 Related Documents
gap	Specific retention periods for assessment records, review decisions and exit certifications are not stated in the information supplied. The procedure defers to the Records Retention and Disposal Policy, whose content was not provided.	Section 7 Records and Register
vague	The incident notification period of 24 hours and the data return or deletion period of 30 days are stated as the organisation's current position or starting point. These are not derived from cited controls and must be confirmed as organisational decisions.	Section 6.6 Step 6
gap	The metrics reporting frequency is not specified in the information supplied. Quarterly is offered as a starting point; the organisation must confirm the appropriate cadence.	Section 8 Metrics

Information the organization must supply

These values were not available from the intake and are required before this document can operate:

- Confirm the incident notification period to be required in AI supplier contracts (24 hours is the current stated position; this is an organisational decision, not a framework requirement).
- Confirm the data return or deletion period to be required at contract exit (30 days is offered as a starting point; this is an organisational decision, not a framework requirement).
- Confirm the metrics reporting frequency (quarterly is offered as a starting point).
- Reconcile this procedure with the actual content of the Third-Party Risk Management Policy, AI Risk Management Standard, Records Retention and Disposal Policy and other referenced documents to ensure thresholds, retention periods and requirements align.
- Confirm whether additional Ontario privacy legislation requirements apply to AI supplier engagements and whether specific contract terms are needed to address them; legal review is recommended.

- Provide or confirm the AI Supplier Intake Form template referenced in Step 1, or confirm that one will be created to capture the required fields.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

SPECIMEN