

**Specimen — illustrative example**

The organisation named in this document is fictional. This document comes from the scenario described on [riskwoven.com/examples](https://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.

# Solstice AI Acceptable Use Policy Operating Procedure

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.

|                 |                                             |
|-----------------|---------------------------------------------|
| Source policy   | Solstice AI Acceptable Use Policy           |
| Document status | Draft for owner and professional review     |
| Owner           | To be assigned                              |
| Review cycle    | At least annually and after material change |

## 1. Purpose

This procedure translates adopted policy requirements into practical instructions. It does not replace the source policy.

## 2. Scope

Applies to employees, contractors, systems and business processes covered by the source policy.

## 3. Roles and responsibilities

- **Policy owner:** records decisions on interpretations, exceptions and material changes.
- **Process owner:** maintains these instructions and confirms controls operate.
- **Users:** follow the instructions and report issues promptly.
- **Reviewer:** checks evidence and escalates gaps.

## 4. Procedure

### 1. Use only AI tools listed in the AI tool register maintained by the Chief Technology Officer

**Responsible party:** Staff

1. The process owner confirms this step applies.
2. The person responsible (Staff) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

### 2. Complete a privacy review before any new tool is added to the AI tool register

**Responsible party:** Privacy Officer

**Applies when:** A new AI tool is proposed for addition to the register.

1. When the condition above arises, the process owner confirms this step applies.
2. The person responsible (Privacy Officer) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

### 3. Maintain the AI tool register

**Responsible party:** Chief Technology Officer

*Implied by the source text rather than stated explicitly — confirm the interpretation with the policy owner.*

1. The process owner confirms this step applies.
2. The person responsible (Chief Technology Officer) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

#### **4. Do not enter customer names, account numbers, meter readings or billing records into any AI tool that is not...**

**Requirement:** Do not enter customer names, account numbers, meter readings or billing records into any AI tool that is not listed in the register as cleared for customer data.

**Responsible party:** Staff and contractors

1. The process owner confirms this step applies.
2. The person responsible (Staff and contractors) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

#### **5. Review any AI output before it is used in a customer communication, a billing adjustment or a disconnection...**

**Requirement:** Review any AI output before it is used in a customer communication, a billing adjustment or a disconnection decision.

**Responsible party:** Named staff member

**Applies when:** An AI output is to be used in a customer communication, a billing adjustment or a disconnection decision.

1. When the condition above arises, the process owner confirms this step applies.
2. The person responsible (Named staff member) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

#### **6. Record the review in the case management system**

**Responsible party:** Reviewer

**Applies when:** A review of an AI output has been completed.

1. When the condition above arises, the process owner confirms this step applies.
2. The person responsible (Reviewer) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

## **7. Where AI outputs are used in load forecasting or outage planning, those outputs should be compared with the...**

**Requirement:** Where AI outputs are used in load forecasting or outage planning, those outputs should be compared with the previous forecasting method for at least three months before they are relied on.

**Responsible party:** Staff and contractors

**Applies when:** AI outputs are to be used in load forecasting or outage planning.

1. When the condition above arises, the process owner confirms this step applies.
2. The person responsible (Staff and contractors) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

## **8. Report any AI output that is wrong, harmful or unexpected to the service desk within one business day**

**Responsible party:** Staff and contractors

**Applies when:** An AI output is identified as wrong, harmful or unexpected.

1. When the condition above arises, the process owner confirms this step applies.
2. The person responsible (Staff and contractors) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

## **9. Review each incident report and decide whether the relevant AI tool is paused**

**Responsible party:** Chief Technology Officer

**Applies when:** An incident report is received from the service desk.

1. When the condition above arises, the process owner confirms this step applies.
2. The person responsible (Chief Technology Officer) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

## **10. Complete the annual AI awareness module**

**Responsible party:** All staff who use AI tools

1. The process owner confirms this step applies.
2. The person responsible (All staff who use AI tools) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

## **11. Confirm completion of the annual AI awareness module for their teams each year**

**Responsible party:** Managers

**Applies when:** The annual AI awareness module cycle concludes.

1. When the condition above arises, the process owner confirms this step applies.
2. The person responsible (Managers) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

## **12. Review this policy every twelve months and after any significant AI incident**

**Responsible party:** Chief Technology Officer

**Applies when:** Twelve months have elapsed since the last review, or a significant AI incident has occurred.

1. When the condition above arises, the process owner confirms this step applies.
2. The person responsible (Chief Technology Officer) carries out the requirement and records that it was done.
3. The reviewer checks the record and escalates any exception to the policy owner.

## **5. Evidence and records**

Keep decisions, completed checklists, review records, exceptions, incidents and corrective actions according to the organisation's retention schedule.

## **6. Exceptions and escalation**

Stop and contact the policy owner when a requirement cannot be met, the activity involves sensitive information, or the potential impact is significant. Record every agreed exception with

an expiry date and compensating controls.

## 7. Review

Review this document when the source policy, related systems, legal obligations or business process changes.

SPECIMEN