

# Risk Assessment Policy

|                |                        |
|----------------|------------------------|
| Owner          | [Security owner role]  |
| Approved by    | [Policy approver role] |
| Effective date | [Effective date]       |
| Next review    | [Next review date]     |
| Version        | [Version]              |

## 1. Purpose and scope

This policy supports the SOC 2 common criteria CC3.1, CC3.2, CC3.3 and CC3.4 by establishing the process for identifying, assessing, and managing information security risks.

The risk management process covers all [In-scope systems], applications, business processes, and third parties.

## 2. Annual risk assessment

A formal risk assessment is conducted at least annually to identify threats, vulnerabilities, and the potential impact on service commitments.

## 3. What the assessment considers

- The Company objectives and the commitments made to customers.
- Threats and weaknesses in the systems in scope, including those found by vulnerability scans and tests.
- Vendors and subservice organizations, and what they can reach.
- Fraud and misuse by insiders, including how a control could be overridden.
- Changes since the last assessment: new products, systems, vendors, locations and staff.

## 4. Scoring

Each risk is rated for likelihood and impact on a scale of 1 to 5. The score is likelihood multiplied by impact, from 1 to 25, and higher scores are treated first.

| Rating | Likelihood                           | Impact                                  |
|--------|--------------------------------------|-----------------------------------------|
| 1      | Not expected in the next three years | Minor inconvenience, no customer effect |

| Rating | Likelihood                           | Impact                                                        |
|--------|--------------------------------------|---------------------------------------------------------------|
| 2      | Could happen in the next three years | Limited internal disruption                                   |
| 3      | Could happen in the next year        | Some customers affected or a contract breached                |
| 4      | Expected in the next year            | Customer data exposed, or the service down for every customer |
| 5      | Expected within months               | Severe harm to customers or the business                      |

## 5. Risk register

All identified risks are tracked in a central [Risk register location]. Each entry includes a description, likelihood, impact, risk rating, owner, and treatment plan.

## 6. Risk treatment

Risks are treated by accepting, mitigating, transferring, or avoiding them. Mitigation plans are tracked to completion.

A risk is accepted only by the [Policy approver role], in writing, with the date of acceptance and a date to look at it again. The person who identified a risk does not accept it.

## 7. Reassessment between reviews

A significant change triggers a reassessment of the risks it touches before or as it happens: a new subservice organization, a major architecture change, a new product or market, a serious incident, or a change in the team that owns key controls. Results are reported to the [Management review body].

## 8. Roles and responsibilities

| Role            | Held by                | Responsibility                                                                                                         |
|-----------------|------------------------|------------------------------------------------------------------------------------------------------------------------|
| Policy approver | [Policy approver role] | Approves this policy, each new version, and any risk the Company accepts instead of meeting it.                        |
| Policy owner    | [Security owner role]  | Maintains this policy, makes sure the controls in it operate, keeps the evidence, and reviews it at least once a year. |
| All personnel   | Everyone in scope      | Follow this policy and report a suspected breach of it to the [Security owner role].                                   |

## 9. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

| Record                  | What it shows                                                    | Where it is kept            |
|-------------------------|------------------------------------------------------------------|-----------------------------|
| Approved policy         | This document, signed by the approver, with its version history. | [Documentation system]      |
| Risk assessment report  | Annual assessment findings and results.                          | [Evidence storage location] |
| Risk register           | All identified risks with their status.                          | [Risk register location]    |
| Risk acceptance records | Each accepted risk with its approver, date and revisit date.     | [Risk register location]    |

## 10. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

## 11. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

| Version   | Date             | Summary of change | Approved by            |
|-----------|------------------|-------------------|------------------------|
| [Version] | [Effective date] | First version.    | [Policy approver role] |
|           |                  |                   |                        |

### Policy approver

Name:

---

Signature:

---

Date:

---

## 12. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

| Field                       | What to enter                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------|
| [Company name]              | Your legal company name.                                                                        |
| [Effective date]            | The date the approver signs this version.                                                       |
| [Version]                   | Start at 1.0 and increase it each time the document changes.                                    |
| [Security owner role]       | The role that runs the security program day to day, for example Chief Technology Officer.       |
| [Policy approver role]      | The officer who approves policies and accepted risks, for example Chief Executive Officer.      |
| [Management review body]    | The group that oversees security, for example the leadership team meeting or an advisory board. |
| [Evidence storage location] | The shared folder or system where evidence is kept.                                             |
| [Documentation system]      | Where policies and procedures are published, for example the company wiki.                      |
| [In-scope systems]          | The product, cloud accounts and tools inside the audit boundary.                                |

| Field                       | What to enter                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------|
| [Risk register location]    | Where the risk register is kept.                                                       |
| [Evidence retention period] | How long audit evidence is kept, for example three years.                              |
| [Next review date]          | The date this version must be reviewed by, at most 12 months after the effective date. |

## Source

Source: free template from [www.polaralabs.com/templates/risk-assessment-policy](http://www.polaralabs.com/templates/risk-assessment-policy) (CC BY 4.0).