GOOD SECURITY

Security Questionnaire Response Pack

Evidence-backed answers, domain structure, and explicit follow-up items where judgement is required.

CLIENT	QUESTIONNAIRE	PROFILE
Kiwi Manufacturing Ltd	**Security Due Diligence Review 2026**	**SME standard**

RESPONSES	AVERAGE CONFIDENCE	MANUAL REVIEW
20	**89%**	**1**

RESPONSE PACK STANDARD

This example shows the level of response pack we would use for lower-risk customers, insurers, and practical due-diligence requests. It still includes full section coverage, evidence references, and explicit follow-up items where human confirmation is needed.

Executive summary

Kiwi Manufacturing Ltd is responding to Security Due Diligence Review 2026 with 20 answered questions across 5 control domains. Average confidence is 89%, with 1 items flagged for human confirmation before final submission.

The pack is designed to let a buyer review the control story quickly while still giving the delivery team a traceable answer set, linked evidence, and explicit follow-up points.

Questionnaire scope and assumptions

Answers assume current production controls and documented practices as at the sample generation date. Where a question requires contractual confirmation, supplier evidence, or consultant judgement, the response is still surfaced with a clear manual-review note rather than being silently omitted.

Domain summaries

Domain	Questions	Approved	Manual review	Average confidence
Identity & Access Management	4	4	0	90%
Asset / Endpoint Security	4	4	0	90%
Data Security & Privacy	4	4	0	90%
Threat / Vulnerability / Incident Management	4	3	1	83%
Business Continuity / Backup / Recovery	4	4	0	90%

Identity & Access Management

4 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
Do you enforce MFA for workforce and administrative access to cloud services?	Yes. MFA is enforced through Microsoft Entra ID Conditional Access for all workforce access, with stronger controls applied to administrative roles.	90%	Approved
How do you control privileged access?	Privileged access is limited to named administrators, approved through change control, and reviewed quarterly. Break-glass credentials are separately logged and tested.	90%	Approved
How quickly is access removed when someone leaves or changes role?	Workforce access is removed or adjusted on the same day the HR event is confirmed, with service desk verification against the joiner / mover / leaver workflow.	90%	Approved
Do you use SSO for core business applications?	Yes. Core SaaS platforms including Microsoft 365, Xero, Employment Hero, and Azure-hosted services are integrated with Entra ID SSO.	90%	Approved

Asset / Endpoint Security

4 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
How do you maintain endpoint protection across laptops and workstations?	All managed corporate endpoints run Sophos XDR with central policy enforcement, alerting, and tamper protection. Exceptions are tracked and reviewed monthly.	90%	Approved
Do you apply a standard configuration baseline to endpoints?	Yes. Microsoft Intune configuration profiles, disk encryption, and browser hardening baselines are applied to managed laptops and desktops.	90%	Approved
How do you manage vulnerabilities on endpoints?	Endpoints are patched through Intune and vendor tooling, with exposure tracked through the monthly posture report and escalated where remediation falls outside SLA.	90%	Approved

Question	Answer	Confidence	Review
Are unmanaged or legacy endpoints identified separately?	Yes. Legacy OT-adjacent devices and unsupported handhelds are tracked separately in the asset register so compensating controls can be documented and reviewed.	90%	Approved

Data Security & Privacy

4 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
How do you classify and protect sensitive information?	Sensitive information is covered by a simple classification model and M365 controls for access restriction, retention, and information handling.	90%	Approved
Do you operate formal retention and deletion controls for personal information?	Retention periods are defined for core records, and deletion or archival actions are tracked through the privacy operating cadence rather than left to manual judgement.	90%	Approved
How do you manage cross-border disclosure and privacy obligations?	Cross-border disclosures are identified in the data inventory and reviewed against Privacy Act expectations before new vendors or transfers are approved.	90%	Approved
Do you have email and collaboration controls to reduce accidental data loss?	Yes. Data loss prevention controls and sharing restrictions are applied to the core Microsoft 365 tenant, with priority rules for personal and financial information.	90%	Approved

Threat / Vulnerability / Incident Management

4 representative questions in this domain. 1 need human follow-up.

Question	Answer	Confidence	Review
How are security incidents detected and escalated?	Managed detection tooling, service desk escalation paths, and a documented incident workflow are used to triage and escalate security events.	90%	Approved
Do you maintain a documented incident response process?	Yes. The business has an incident response plan, breach-notification steps, and role-based decision points covering containment, communication, and recovery.	90%	Approved
How do you track and remediate vulnerabilities that cannot be fixed immediately?	Open vulnerabilities are risk-ranked, given named owners, and monitored through the monthly and quarterly governance cadence until remediation or compensating control sign-off.	90%	Approved
Do you complete independent security testing?	Independent testing is scheduled through the annual assurance plan, but the sample statement below still requires the final 2026 scope confirmation before it would be submitted to a...	61%	Manual review

Business Continuity / Backup / Recovery

4 representative questions in this domain. 0 need human follow-up.

Question	Answer	Confidence	Review
Do you maintain tested backup and recovery arrangements?	Yes. Critical systems are backed up daily with off-site protection, and restoration is tested against agreed recovery expectations rather than assumed to work.	90%	Approved
How do you plan for operational disruption and business continuity?	Business continuity priorities, critical systems, and escalation responsibilities are documented so production, finance, and customer commitments can be recovered in a managed order.	90%	Approved
Are backup exceptions and recovery dependencies visible to leadership?	Yes. Exceptions are surfaced through the reporting cadence, including systems with legacy constraints or supplier dependencies that affect recovery confidence.	90%	Approved
Do you exercise incident and continuity scenarios?	Tabletop exercises are scheduled as part of the annual assurance plan, and lessons from each exercise are captured into the remediation backlog and board reporting pack.	90%	Approved

Implementation notes / shared-responsibility clarifications

Question	Implementation note / shared responsibility
How do you control privileged access?	Clarified break-glass control and quarterly review cadence.
Do you complete independent security testing?	Confirm the final 2026 independent-testing statement before customer submission.

Evidence references appendix

Question	Evidence references
Do you enforce MFA for workforce and administrative access to cloud services?	Access Management Policy v2.3, Conditional Access Standard v1.8
How do you control privileged access?	Privileged Access Procedure v1.6, Quarterly Access Review Record - Q1 2026
How quickly is access removed when someone leaves or changes role?	Workforce Access Governance Standard v1.4, HR Offboarding Checklist v3.1
Do you use SSO for core business applications?	Identity Architecture Overview 2026, Entra Application Register
How do you maintain endpoint protection across laptops and workstations?	Endpoint Security Standard v2.0, Sophos Central Estate Report - March 2026
Do you apply a standard configuration baseline to endpoints?	Endpoint Baseline Standard v1.9, Intune Compliance Dashboard
How do you manage vulnerabilities on endpoints?	Vulnerability Management Procedure v1.5, Monthly Security Posture Report - February 2026
Are unmanaged or legacy endpoints identified separately?	Information Asset Register - March 2026, Legacy Device Exception Log
How do you classify and protect sensitive information?	Information Classification Standard v1.3, Microsoft 365 Protection Configuration
Do you operate formal retention and deletion controls for personal information?	Personal Data Inventory - March 2026, Retention Schedule v1.2
How do you manage cross-border disclosure and privacy obligations?	Privacy Impact Assessment - ERP Migration, Cross-Border Transfer Register
Do you have email and collaboration controls to reduce accidental data loss?	Data Protection Standard v1.4, M365 DLP Policy Set
How are security incidents detected and escalated?	Incident Management Standard v1.7, Monitoring and Escalation Matrix
Do you maintain a documented incident response process?	Incident Response Playbook Suite v2.1, Privacy Breach Readiness Review

Question	Evidence references
How do you track and remediate vulnerabilities that cannot be fixed immediately?	Risk Register - March 2026, Quarterly Security Scorecard - Q1 2026
Do you complete independent security testing?	Annual Assurance Plan 2026
Do you maintain tested backup and recovery arrangements?	Backup and Recovery Standard v1.5, Quarterly Restore Test Record - February 2026
How do you plan for operational disruption and business continuity?	Business Continuity Plan v1.4, Operational Recovery Priorities
Are backup exceptions and recovery dependencies visible to leadership?	Quarterly Security Scorecard - Q1 2026, Recovery Dependency Register
Do you exercise incident and continuity scenarios?	Annual Assurance Plan 2026, Exercise Improvement Register

Manual-review / unresolved items

Question	Why it needs confirmation	Follow-up
Do you complete independent security testing?	The exact 2026 penetration-test scope and supplier statement still require consultant confirmation.	Confirm the final 2026 independent-testing statement before customer submission.