# Supplier Security Obligations: A Self-Assessment Checklist

**For Malaysian businesses that supply goods or services to other organisations**

*Work through this with your actual contract in front of you. It takes about 30 minutes. Nothing here is submitted to anyone — it's for you.*

---

## Before you start

Get the **most recent signed agreement or renewal** with a customer whose business matters to you — start with the relationship you would least want to lose. If you have several, do this once for each; their terms will differ.

*(A note on why: you cannot tell from the outside which organisations have been designated as NCII entities — that register is not public. So this isn't about picking your biggest customer on the assumption they're designated. It's about starting where the consequences of a problem would be greatest for you.)*

You are looking for what you have **promised**, and whether you could **prove** it.

---

## Part A — Does any of this apply to me?

| | Question | Answer |
|---|---|---|
| A1 | Has your business received a formal designation letter naming you a National Critical Information Infrastructure (NCII) entity? | ☐ Yes ☐ No |
| A2 | Do you supply goods or services to an organisation operating in one of the eleven listed sectors — government, banking and finance, transport, defence, information/communication/digital, healthcare, water, energy, agriculture, trade and industry, or science and technology? | ☐ Yes ☐ No |
| A3 | In doing so, do you handle, store, transmit or have access to **their** data — especially personal data of their customers or patients? | ☐ Yes ☐ No |
| A4 | Do you connect to their systems, or send them files containing personal data? | ☐ Yes ☐ No |

**How to read your answers:**

- **A1 = Yes** → You have direct statutory duties under the Cyber Security Act 2024. This checklist is not enough; you need the full obligation set.
- **A1 = No, and A2 + (A3 or A4) = Yes** → **This checklist is for you.** Your customer's compliance duties will reach you through your contract, whether or not anyone has said so.
- **A2 = No** → The Cyber Security Act very likely doesn't affect you at all, and neither do the contract-driven security obligations this checklist covers. You can stop here with a clear conscience. *(Data-protection law may still apply to you separately — see the note below — but that is a different matter from the security duties assessed here.)*

---

**A note on data protection (the PDPA) — separate from this checklist.**

A few of the clauses below (B1 and B8 especially) exist because you handle *personal* data, and they trace back to a different law — the **Personal Data Protection Act (PDPA)**, not the Cyber Security Act. The PDPA is its own regime, with its own regulator and its own specialists. This checklist is about your **security** readiness: whether you can protect, control and account for the data and systems you've been trusted with. It does **not** assess PDPA compliance — consent records, privacy notices and data-retention are a separate exercise for a data-protection adviser or lawyer. Keep the two distinct, and don't let one stand in for the other.

---

# Part B — Find the obligations in your contract

Look for sections with these headings, or wording like them. Tick what your contract actually contains.

| | Look for | Present ? | Clause no. |
|---|---|---|---|
| B1 | **Personal data protection** — a clause requiring PDPA compliance | ☐ | |
| B2 | **Security measures** — often worded "appropriate technical and organisational measures" | ☐ | |
| B3 | **Confidentiality / NDA** — restrictions on disclosing information | ☐ | |
| B4 | **Breach or incident notification** — a duty to tell your customer if something goes wrong, often with a deadline | ☐ | |
| B5 | **Audit rights** — the customer may inspect, audit or assess you | ☐ | |
| B6 | **Certification warranty** — you hold, or will obtain, ISO/IEC 27001 or "an equivalent framework" | ☐ | |

| | | | |
|---|---|---|---|
| B7 | **Sub-contracting restrictions** — you may not pass work or data to third parties without written approval | ☐ | |
| B8 | **Consent warranties** — you confirm you hold consent from the individuals whose data you handle | ☐ | |
| B9 | **Indemnity** — you cover your customer's losses, fines or penalties if you breach the above | ☐ | |

**If B9 is present**, note it: an indemnity turns every other gap on this list into direct financial exposure. It is the clause that gives the rest their teeth.

**If you ticked nothing**, check whether your agreement refers to a separate schedule, addendum, or "supplier code" — obligations often sit there rather than in the main body.

---

# Part C — The evidence test

This is the part that matters. For each obligation you found, the question is **not** "do we do this?" It is:

> **If my customer audited me next month and asked for proof, what would I hand them?**

A claim is *"we keep data secure."* Evidence is a document, dated and followed. Work through each one honestly.

## C1 — Security measures (against B2)

| | Question | Yes | No | Not sure |
|---|---|---|---|---|
| a | Do you have a **written** data security or information security policy? | ☐ | ☐ | ☐ |
| b | Is it **dated**, and has it been reviewed in the last 12 months? | ☐ | ☐ | ☐ |
| c | Could you name who is responsible for it? | ☐ | ☐ | ☐ |
| d | Do your staff know it exists? | ☐ | ☐ | ☐ |

## C2 — Handling and sending data

| | Question | Yes | No | Not sure |
|---|---|---|---|---|
| a | When you send files containing personal data, are they **encrypted or password-protected**? | ☐ | ☐ | ☐ |

| | | | | |
|---|---|---|---|---|
| b | Is customer data handled in accounts your **business controls** — where someone can revoke access, transfer ownership, and produce access logs — rather than in an individual's personal account? | ☐ | ☐ | ☐ |
| c | Do you know **where** customer or patient data is stored — which system, which folder, whose device? | ☐ | ☐ | ☐ |
| d | Could you list **who has access** to it? | ☐ | ☐ | ☐ |
| e | Is access removed **the day** someone leaves? | ☐ | ☐ | ☐ |
| f | Is multi-factor authentication (MFA) enabled on your email and any cloud storage holding customer data? | ☐ | ☐ | ☐ |

**On question (b) — a common misunderstanding.** This is not about consumer email being technically weaker. A personal Gmail account may well have stronger transport encryption and better multi-factor authentication than a small business's own mail server.

The issue is **control and custody**, not encryption:

- **Revocation.** If the account belongs to an individual, the business cannot remove access when that person leaves. They walk out with the data still in their inbox. That directly defeats question (e).
- **Audit.** A business account has an administrator who can produce access logs. A personal account cannot show an auditor who accessed what, and when.
- **Continuity.** If the account holder is unavailable, or falls out with the business, the business has no route to the data.
- **Contractual paperwork.** Business email services offer data-processing terms; consumer accounts are governed by consumer terms, with no equivalent arrangement covering data you handle on a customer's behalf.
- **Mixing.** A personal inbox holds private correspondence alongside customer data, which complicates retention, deletion and any investigation.

So the test isn't "is it Gmail?" It's **"can the business demonstrate control over the account, and prove who has had access?"**

## C3 — Data-protection and consent clauses (against B1, B8)

If your contract carries the clauses at B1 or B8, you also have **data-protection obligations** — consent, privacy notices, how long you keep personal data and how you dispose of it. These are real and worth taking seriously.

But they belong to a **different regime** from the security duties this checklist assesses (see the note after Part A). Whether your consent records, privacy notices and retention practices actually satisfy the PDPA is a separate exercise, and the right person for it is a **data-protection adviser or lawyer** — not a security gap-assessment. This checklist doesn't score them; it simply flags that they exist so you don't overlook them.

## C4 — Incidents (against B4)

| | Question | Yes | No | Not sure |
|---|---|---|---|---|
| a | Do your staff know who to tell if a laptop is lost, an email goes to the wrong person, or an account is compromised? | ☐ | ☐ | ☐ |
| b | Do you have a **written note of what you would do** in that situation? | ☐ | ☐ | ☐ |
| c | Do you know the **deadline** your contract gives you for telling your customer? | ☐ | ☐ | ☐ |
| d | Do you keep a record of incidents, however minor? | ☐ | ☐ | ☐ |

## C5 — Certification (against B6)

| | Question | Yes | No | Not sure |
|---|---|---|---|---|
| a | If your contract says you hold ISO/IEC 27001 or an equivalent — **do you actually hold it?** | ☐ | ☐ | ☐ |
| b | If it says "or equivalent framework," could you show what your equivalent is? | ☐ | ☐ | ☐ |

## C6 — Third parties (against B7)

| | Question | Yes | No | Not sure |
|---|---|---|---|---|
| a | Can you list every outside party — IT support, software vendors, cloud services, freelancers — who can reach your customer's data? | ☐ | ☐ | ☐ |
| b | Has your customer approved them in writing, where the contract requires it? | ☐ | ☐ | ☐ |

## C7 — Licensed services

| | Question | Yes | No | Not sure |
|---|---|---|---|---|
| a | Do you buy or provide **managed SOC monitoring** or **penetration testing**? | ☐ | ☐ | ☐ |
| b | If yes — does the provider hold a **NACSA licence**? | ☐ | ☐ | ☐ |

*These two services require a licence under P.U.(A) 221/2024. Most other security work — risk assessments, policy work, advisory, training — does not.*

# Part D — Where you stand

Count your answers across Part C.

**Mostly "Yes"** — You're in reasonable shape. Your remaining task is making sure the documents are current and that someone owns keeping them that way. Re-run this checklist after your next contract renewal.

**A mix of "Yes" and "No"** — Normal, and manageable. Start with the "No" answers in **C1** and **C2**: a written policy and secure data handling are the two things a customer asks for first, and they're the cheapest to fix.

**Mostly "No" or "Not sure"** — You have obligations in a signed contract that you cannot currently evidence. Nothing has gone wrong yet, and this is a fixable position — but it's worth addressing before your customer asks rather than after.

**Any "Not sure" is worth treating as a "No"** for now. If you can't answer confidently in your own office, you won't answer confidently in an audit.

---

# What this checklist cannot tell you

Being straight about the limits.

This checklist tells you **whether you have something**. It cannot tell you whether what you have would **survive scrutiny** — because you can't objectively test your own evidence. Auditors test three things a self-assessment can't:

1. **Is the document actually followed?** A policy nobody reads is evidence of nothing.
2. **Is "appropriate" appropriate for you?** The standard is proportionate to your size, your data, and your risk — and judging that requires an outside view.
3. **Does the evidence match the specific words of your clause?** Contracts differ. A policy that satisfies one customer's wording may not satisfy another's.

That gap — between *"we said yes"* and *"we can prove yes"* — is where an assessment adds something a checklist can't.

---

# If you'd like a second pair of eyes

I run fixed-scope, fixed-fee contract assessments: I read your agreement, map every obligation it places on you, test each against what you could actually evidence, and give you a prioritised gap report and a call to go through it.

If closing a gap needs **penetration testing** or **managed SOC monitoring**, those are licensed services and I don't hold that licence — I'll tell you what's needed and refer you to someone who does.

**Kenneth Wong** · kenneth@chuinwei.com · chuinwei.com

---

*This checklist is educational and is not legal advice. It describes obligations as they commonly appear in supplier contracts and does not assess your specific agreement. Where a decision carries real consequences, take proper advice.*