Data Breach Response Plan

VERSION	Version 2 (published)
CREATED	5 November 2026
PUBLISHED BY	Copied from Sky5G Australia v2
ONLINE	https://sky5g.global/legal/data-breach

Sky5G Australia Data Breach Response Plan

Updated: 4 November 2026

AI-produced draft (version 1) — requires review by Australian privacy counsel before it is relied on. Names in [square brackets] are placeholders to be filled in.

We hold information that matters: who our customers are, how to contact and bill them, which services and SIMs they have, where their fixed wireless equipment is, identity documents we check at signup, and the telecommunications data the law requires us to keep. If any of that is lost, stolen, exposed or misused, people can be harmed — financially, physically or through loss of trust. This plan sets out how **Wi-Sky Queensland Pty Ltd (ABN 91 613 554 546), trading as Sky5G Australia**, prepares for, responds to and learns from a data breach, and how we meet the **Notifiable Data Breaches (NDB) scheme** in Part IIIC of the *Privacy Act 1988* (Cth).

1. Purpose and scope

This plan applies to every data breach, suspected or confirmed, involving personal information or other confidential information that Sky5G Australia holds or controls, wherever it sits: our platform and databases, the mobile core and RADIUS systems, backups, laptops and phones, paper, resellers and contractors, and cloud or software providers acting for us.

It covers all staff, contractors, resellers and field technicians working for Sky5G Australia. It sits alongside our Privacy Policy, Network Outage Policy, Complaints Handling Process, our staff training on privacy, cyber security and confidential information, and our security obligations as a carriage service provider.

Objectives:

- contain a breach fast and limit the harm to the people affected;
- assess it honestly and within the time the law allows;
- tell the people affected, the Office of the Australian Information Commissioner (OAIC) and other authorities when the law requires it, and whenever doing so helps people protect themselves;
- keep a complete record; and
- fix the cause so it does not happen again.

2. Definitions

- **Personal information** — information about an identified or reasonably identifiable individual, as defined in the Privacy Act. For a telco this includes names, contact details, dates of birth, identity document details, payment details, account notes, call and data records, location information (including cell-site location information and fixed wireless service addresses), IP address assignments and the data we retain under Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (which section 187LA treats as personal information).
- **Sensitive information** — a subset with stronger protection: health information (for example hardship or vulnerability notes), information about domestic or family violence circumstances, biometric data used for identity checks, racial or ethnic origin, and similar.
- **Data breach** — unauthorised access to, unauthorised disclosure of, or loss of personal information we hold. Examples: a database or backup exposed to the internet, a laptop or phone lost, an email sent to the wrong customer, a staff member looking up a customer without a business reason, a reseller sharing a customer list, ransomware, a phishing compromise of a staff account, a SIM swap carried out on forged identity.
- **Eligible data breach** — a data breach where (a) there is unauthorised access to, disclosure or loss of personal information, (b) a reasonable person would conclude it is **likely to result in serious harm** to any of the individuals concerned, and (c) we have not been able to prevent that likely serious harm through remedial action. Eligible data breaches must be notified to the OAIC and to affected individuals.
- **Serious harm** — physical, psychological, emotional, financial or reputational harm. Relevant factors (section 26WG of the Privacy Act) include the kind and sensitivity of the information, whether it was protected (for example encrypted) and how easily that protection could be overcome, who obtained or could obtain it, and the nature of the harm.
- **Response team** — the people named in section 3 who run the response.
- **Breach register** — the record described in section 8.

3. Roles and the response team

Role	Who	Responsibilities
Incident lead	[Chief Technology Officer / name] Â— deputy: [name]	Declares an incident, owns the response plan for that incident, chairs response meetings, decides containment actions, keeps the timeline, briefs the Privacy Officer and directors
Privacy Officer	[name, privacy@sky5g.com.au]	Runs the assessment (section 5), decides with the Incident lead and legal adviser whether the breach is eligible, prepares and lodges the OAIC statement, owns the breach register
Technical lead	[Head of Network / Platform Engineering]	Investigates, preserves evidence, contains and eradicates the cause, restores systems, coordinates with vendors (cloud, core network, SIM supplier)

Communications lead	[name]	Customer, staff, reseller and media communications; status page and website notices; call-centre scripts
Legal adviser	[external privacy counsel]	Advises on eligibility, regulator and law-enforcement notifications, contractual notifications, insurance
Customer care lead	[Support manager]	Handles affected customers' calls and chats, identity re-verification, SIM and account protection, hardship and vulnerability cases
Director sponsor	[Managing Director]	Approves notifications and public statements, informs insurers and the board

Every staff member, contractor and reseller must report a suspected breach **immediately** — within the hour — to the Incident lead or Privacy Officer by phone or the #security-incidents channel, and must not try to investigate, delete evidence or contact affected people themselves. Nobody will be penalised for reporting in good faith, including their own mistake.

4. Severity classification

Level	Description	Examples	Response
S1 Â— Critical	Large-scale or highly sensitive exposure; likely serious harm; ongoing attacker access; identity documents, payment data, location data or DFSV-flagged records involved; or a cyber security incident with significant impact on service	Database exfiltration; ransomware; identity-document store exposed; SIM swap fraud wave	Response team convened within 1 hour, 24/7; director sponsor informed at once; daily (or more frequent) updates; legal adviser engaged immediately
S2 Â— Major	Moderate numbers or sensitivity; harm possible; access contained	Lost unencrypted laptop with customer exports; bulk mis-addressed email with account details; reseller mishandling a customer list	Response team convened within 4 hours; assessment started the same business day
S3 Â— Minor	Few people, low sensitivity, quickly contained, harm unlikely	One mis-sent invoice; a single mis-filed note; a look-up without a business reason where nothing was copied or shared	Handled by the Privacy Officer with the business owner; logged; assessed within 5 business days
S4 Â— Near miss	No personal information actually accessed, disclosed or lost	Blocked phishing attempt; misconfiguration found before exposure	Logged and reviewed for lessons; no notification

Severity can move up or down as facts emerge. When in doubt, treat the incident as the higher level.

5. The five phases

Phase 1 Â— Contain (immediately; first 24 hours)

1. Record the time of discovery and who reported it. Open an entry in the breach register and start the incident timeline.
2. Stop the breach: revoke or reset compromised credentials and sessions, isolate affected systems, block the exfiltration path, recall a mis-sent message where possible, remotely wipe lost devices, suspend a reseller's or staff member's access, take an exposed bucket or endpoint offline.
3. Preserve evidence: snapshot logs, images and access records before changing anything else; do not delete emails or messages; note every action taken and when.
4. Protect customers at risk: for SIM-swap or account-takeover exposure, lock the affected accounts, require re-verification for porting and SIM changes, and alert the fraud queue. For location or DFSV-related information, involve the Customer care lead at once so at-risk customers can be contacted safely (see our Domestic, Family & Sexual Violence Policy).
5. Decide whether we are also dealing with a **cyber security incident** reportable under the *Security of Critical Infrastructure Act 2018* or a ransomware demand reportable under the *Cyber Security Act 2024* (section 6) — those clocks start now.

Phase 2 Â— Assess (as quickly as possible; completed within 30 days of becoming aware)

The Privacy Act gives us **at most 30 calendar days** from when we become aware there are reasonable grounds to suspect an eligible data breach to complete a reasonable and expeditious assessment. We aim to finish well inside that: within 5 business days for S1 and S2.

The assessment records:

- what happened, how, and when — and whether it is over;
- the information involved: what kinds, how many people, which systems, whether sensitive information or identity documents are included, whether it was encrypted or otherwise protected;
- who has or could have the information, and what they could do with it;
- the likely harm to the people concerned and how serious it would be — considering their circumstances, including customers known to be vulnerable;
- whether remedial action has prevented the likelihood of serious harm for all, some or none of them (if it has for all of them, the breach is not eligible, and we record why);
- our conclusion: **eligible** or **not eligible**, signed off by the Privacy Officer and the Incident lead with the legal adviser's advice.

If the assessment is not finished within 30 days we record why and keep going; the delay itself is reported to the OAIC with the statement.

Phase 3 Â— Notify (as soon as practicable after the assessment)

If the breach is eligible, or we otherwise decide notification is right, we notify:

- **The OAIC** — by lodging the *Notifiable Data Breach form* on the OAIC website with the information required by section 26WK: our identity and contact details, a description of the breach, the kinds of information concerned, and the steps we recommend individuals take. Where another organisation (for example a cloud provider or reseller) holds the same information jointly, we agree which entity notifies so that one statement covers it.

- **Affected individuals** — using one of the three options in the Act, in this order of preference: (1) each affected individual directly; (2) only those at risk of serious harm; or (3) if neither is practicable, publish the statement on our website and take reasonable steps to publicise it. We tell customers by email and SMS to their verified contact details, in plain English, and in another language on request. For customers flagged as vulnerable or with a DFSV safety flag, the Customer care lead decides the safe channel first.
- **Law enforcement and security agencies** — the Australian Cyber Security Centre (ReportCyber) for cyber incidents; the police where a crime is involved; the relevant Commonwealth agency where retained telecommunications data or interception capabilities are affected.
- **Other authorities and parties as required** — the ACMA and the Telecommunications Industry Ombudsman (TIO) where the breach affects consumer protections or complaints are likely; the Australian Signals Directorate under the SOCI Act for significant cyber incidents (section 6); card schemes and our payment provider for payment data; our insurer; and any wholesale carrier, SIM supplier or platform vendor whose systems are implicated.
- **Staff and resellers** — what happened, what to say to customers, and what not to say, before customers are told.

Notification may be delayed only to the extent the law allows — for example where a law-enforcement agency asks us to, or where it would prejudice the security of the affected systems. The reason and the agency's request are recorded.

Timelines we hold ourselves to:

Audience	Target
OAIC statement	As soon as practicable after concluding eligibility; never later than the day the assessment is completed plus 3 business days
Affected individuals	As soon as practicable after the OAIC statement is prepared; same day as lodgement wherever possible
ASD / ACSC (SOCI cyber incident)	12 hours if the incident has, or is having, a significant impact on service availability; 72 hours for other relevant impacts
Ransomware payment report (if one were ever made)	72 hours
Staff and resellers	Before customer notification goes out

Phase 4 Â— Review (within 30 days of closing the incident)

A post-incident review, led by the Privacy Officer with the Technical lead, covering root cause, what worked and what did not in this plan, the completeness of our logging and evidence, whether our security controls, access rights, training or supplier contracts need to change, and whether a wider privacy impact assessment is warranted. Actions are assigned owners and dates and tracked to completion. Findings are reported to the directors.

Phase 5 Â— Record

Every incident — including near misses and breaches we assess as not eligible — is recorded in the breach register (section 8) with the assessment and its reasoning, so we can show the OAIC that we complied with the scheme even where we decided not to notify.

6. Related legal obligations we track alongside the NDB scheme

- **Security of Critical Infrastructure Act 2018** — as a carrier / carriage service provider our assets may be critical infrastructure assets; cyber security incidents with a significant impact on availability must be reported to the ASD within **12 hours**, and other relevant impacts within **72 hours**, with a written report following. [Confirm applicability with counsel; record the asset register reference here.]
- **Cyber Security Act 2024** — a ransomware or cyber extortion payment must be reported within **72 hours** of making it. Our position is that we do not pay ransoms without director and legal sign-off.
- **Telecommunications Act 1997, Part 13 and Part 14** — confidentiality of customer information and carrier security obligations, including notifying the Communications Access Co-ordinator of changes that affect security.
- **Telecommunications (Interception and Access) Act 1979, Part 5-1A** — retained data is personal information; its confidentiality and the integrity of the retention system must be protected and breaches treated as NDB matters.
- **TCP Code and the TIO scheme** — complaints arising from a breach are handled under our Complaints Handling Process; the TIO can be contacted on 1800 062 058.
- **Australian Consumer Law and our contracts** — some customer and wholesale contracts require notification within fixed times; the legal adviser checks these in Phase 2.

7. Notification templates

Templates live in the admin portal's message templates under data_breach_ *so each is reviewed and translated once. The substance of each:*

To affected customers (email / SMS / letter)

> *Subject: Important information about your Sky5G account Hello [name]. On [date] we found that [plain description of what happened]. The information involved was [what]. [Information that was NOT involved, e.g. "Your payment card details were not affected."] We have [what we have done]. We recommend you [specific steps: change passwords, watch for unexpected SMS codes, contact IDCARE on 1800 595 160, place a credit ban]. We are sorry this happened. We have told the Office of the Australian Information Commissioner. If you have questions call 1300 413 798 or reply to this email; our team will never ask for your password or a code. — Sky5G Australia (Wi-Sky Queensland Pty Ltd)*

To the regulator (OAIC Notifiable Data Breach form) — the identity and contact details of Wi-Sky Queensland Pty Ltd; the Privacy Officer's name and contact; a description of the breach including when it occurred and when we became aware; the kinds of information; the number of individuals; the recommendations to individuals; whether other entities are involved; the steps we have taken.

To staff and resellers

> *We are responding to a data incident affecting [scope]. Do not discuss it outside Sky5G or on social media. If a customer asks, say: "We are aware of an incident and are contacting affected customers directly. I can confirm whether your account is affected / I will arrange a call back from our privacy team." Do not reset a customer's details, port a number or swap a SIM without the enhanced verification steps circulated today. Report anything unusual to [channel].*

8. Register of breaches

The Privacy Officer keeps the breach register (in the admin portal's compliance area, access restricted and audited). Each entry records: reference; date and time discovered and reported, and by whom; description;

systems and information involved; number and categories of individuals; severity; containment actions and timeline; assessment, conclusion and reasoning; notifications made (to whom, when, how, copies); remedial actions and owners; review findings; closure date. Entries are kept for at least **7 years**.

9. Testing, training and review

- Every staff member completes the privacy & data handling and cyber security awareness training modules on joining and yearly; the response team also completes an incident-response walkthrough.
- We run a **tabletop exercise** at least once a year (scenarios: ransomware on the platform, identity-document store exposure, a reseller leak, a SIM-swap fraud wave) and after any major change to our systems.
- This plan is reviewed at least **annually**, after every S1 or S2 incident, and when the law changes. The Privacy Officer owns the review; the directors approve it.

10. Contacts

Who	Contact
Incident lead	[name, mobile, email]
Privacy Officer	[name], privacy@sky5g.com.au, [mobile]
Technical lead	[name, mobile]
Communications lead	[name, mobile]
Legal adviser	[firm, name, phone]
Cyber insurer	[insurer, policy number, 24/7 claims line]
OAIC	1300 363 992 Â— oaic.gov.au (Notifiable Data Breach form)
Australian Cyber Security Centre	1300 CYBER1 (1300 292 371) Â— cyber.gov.au/report
IDCARE (for affected customers)	1800 595 160
Telecommunications Industry Ombudsman	1800 062 058
ACMA	1300 850 115
Police (non-emergency)	131 444

Customers: if you think your Sky5G information has been exposed or misused, call **1300 413 798**, email **support@sky5g.com.au**, or use the chat on our website. If you are unhappy with how we handle it you can complain to us under our Complaints Handling Process, to the TIO, or to the OAIC.