SAMPLE: DATA BREACH NOTIFICATION STATEMENT

As a result of a recent cyber security incident at CS Energy, we are writing to notify you that some of your personal information may have been accessed by, or disclosed to, an unauthorised person.

We take this issue very seriously. We are providing you with this notice so you can take action to protect your information, find support if you need it, and understand what steps CS Energy is taking to investigate this incident. We remain committed to managing your personal information with respect and in accordance with all relevant privacy laws.

If you are a current or former employee or contractor, you may have received an earlier notice about this incident. This is an update to that earlier notice.

What has happened?

As part of a ransomware incident that was first detected on Saturday 27 November 2021, an unauthorised group gained access to our corporate systems and has likely gained access to personal information relating to CS Energy's employees, contractors and job applicants (including students), service providers, and members of the board of directors.

Our investigation shows that the data accessed was dated between September 2000 to August 2010. This may affect you if you were an employee, contractor or job applicant with CS Energy during that period.

CS Energy moved quickly to contain this incident. We immediately notified relevant government agencies, and we worked closely with them and cyber security experts to respond and restore our systems.

The incident occurred on CS Energy's corporate network and did not impact safety or operations at our power stations. There is no indication that the incident was a 'state-based' attack. Our cyber security experts have attributed the attack to a known group of cyber criminals.

Has this information been published on the internet?

There is a possibility that the group behind the incident will release the data publicly or sell it. However, we have been working with cyber security experts and law enforcement to monitor this information, and there is currently no indication that the information has been sold or publicly released.

How could I be affected?

We have identified that affected information may include:

- contact information (name, email address, physical address, home and mobile phone numbers);

- employment information (employment status, company, title, resumes, onboarding reference checks, contact details, salary and redundancy payment information); and
- biographical information (gender, date of birth, maiden name, nationality and residency status).

In very limited cases, it is possible that the data may include:

- certain identification information (passport numbers, tax file numbers, Medicare numbers, driver's licence numbers, vehicle identification numbers and vehicle registration numbers);
- certain financial information (bank account details, superannuation account details); and
- certain health information (workplace injuries, onboarding health checks).

Importantly, the affected information is limited to documents dated between September 2000 and August 2010, and more recent information has not been compromised.

Are the CS Energy systems safe to use or receive information from?

We are confident that our systems are now secure and have taken technical steps to prevent further breach. We are also undertaking a comprehensive review of our systems and implementing measures to update our security procedures.

How can I get support?

If you are concerned about the potential misuse of your personal information, we have arranged free support from IDCARE, Australia's national identity and cybersecurity community support service.

Please engage an IDCARE Case Manager via IDCARE's Get Help Web Form at www.idcare.org/contact/get-help using the **referral code CSN22**.

IDCARE's National Case Management Centre can also be called between 8am and 5pm Monday to Friday AEST (excluding public holidays) on **1800 595 160**.

Alternatively you may visit IDCARE's Learning Centre for further information and resources on protecting your personal information: www.idcare.org/learning-centre.

What should I do?

We recommend that you take steps to ensure your personal information is safeguarded. Some steps to follow include:

(a) Review your accounts for suspicious activity and change your password. Review your salary statements and speak with the payroll team if you see any unexpected changes.

(b) Carefully review your tax, banking and superannuation accounts. In particular, review personal details, any banking details provided and account recovery settings.

(c) If you are concerned your tax file number may have been accessed, contact the Australian Tax Office (ATO) regarding monitoring for unusual activity.

(d) Where possible, ensure that your personal accounts are protected with multi-factor authentication.

(e) Be wary of potential phishing emails and telephone calls requesting personal information (including where the sender or caller appears to know your identity) and avoiding opening unknown attachments. Scams can often impersonate trusted businesses or governments. Wherever possible, make your own enquiries and do not respond to requests to provide your information to unknown people.

(f) Install anti-virus software on your systems and keep it updated.

(g) Apply all recommended software patches for your operating systems and software.

(h) Consider subscribing to the service at http://www.scamwatch.gov.au to receive up to date information on scams in the community.

For general information about how you can you protect your data privacy:

- visit the Australian Competition and Consumer Commission's Scamwatch website at http://www.scamwatch.gov.au;
- read the Australian Cyber Security Centre's resources for personal cyber security: https://www.cyber.gov.au/acsc/view-all-content/advice/personal-security-guides; and
- visit the Office of the Australian Information Commissioner's website, which contains guidance for data breaches at www.oaic.gov.au/individuals/data-breach-guidance and protecting against identity fraud at https://www.oaic.gov.au/privacy/data-breaches/identity-fraud.

You can also contact the Office of the Australian Information Commissioner at www.oaic.gov.au/about-us/contact-us.

Where should I go for more information?

If you have any concerns regarding this security incident, please contact us at Cyberenquiry@csenergy.com.au and we will endeavour to assist as best we can.

Further information about the security incident has been published on our website at https://www.csenergy.com.au/who-we-are/cyber-security. This page may be updated from time to time with new information, so we recommend that you check it regularly.

If new information arises, we will update you either by email or via our website at https://www.csenergy.com.au/who-we-are/cyber-security.

Yours sincerely

Bill Hopsick
Head of Risk, Compliance and Assurance

Brisbane Office
Level 2, HQ North Tower, 540 Wickham Street, Fortitude Valley QLD 4006
PO Box 2227, Fortitude Valley BC QLD 4006

Enquiries: Julie Urquhart, Workplace Relations Specialist
Phone: 0417 697 375
Email: Cyberenquiry@csenergy.com.au