Hudson
Great people. Great performance.

DATA BREACH NOTIFICATION POLICY

Purpose

The purpose of this policy is to enable Hudson to quickly and effectively respond to and manage a suspected or actual data breach in order to protect the personal information we hold, mitigate the potential harm to individuals, minimise the potential impact on our business, our customers and our stakeholders. This policy will also help us to comply with our regulatory obligations under applicable privacy and data protection laws.

Scope

This policy applies to all Hudson staff, including employees, contractors, agents, subcontractors and temporary staff.

What is a data breach?

A data breach occurs when the personal information stored by Hudson is:

- lost;
- accessed, modified or disclosed without permission from the person who provided the information or Hudson; or
- subject to other misuse or interference.

Personal information is information about an identified individual, or an individual who is reasonably identifiable.

Some examples of how data breaches can occur include:

- a disgruntled employee leaking or providing unauthorised access to personal, confidential, or otherwise sensitive information;
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment;
- employees or third party providers inadvertently making public or otherwise disclosing personal information;
- lost or stolen laptops, removable storage devices, or paper records containing personal information;
- hard disk drives or other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased;
- databases containing personal information being 'hacked' or otherwise illegally accessed, including via a phishing attack or business email compromise;

- an internal network being compromised by malicious software (e.g. a ransomware incident);
- paper records stolen from insecure recycling or garbage bins;
- mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address; and
- an individual deceiving Hudson into improperly releasing the personal information of another person.

What should you do if you suspect a breach?

If a staff member becomes aware of an actual or suspected data breach they must immediately notify The Privacy Officer in Hudson's legal team by email at databreachnotice@hudson.com. If possible, that notification should include:

- the time and date at which the actual or suspected breach was discovered;
- the suspected cause and extent of the breach;
- the type of personal information involved;
- how the staff member became aware of the suspected data breach; and
- any relevant context for the affected information and/or the breach.

It is always best to bring a suspected data breach to the attention of the Privacy Officer, even if you are unsure whether the situation qualifies as a data breach.

Staff members **must not** notify any individuals or third parties (including privacy regulators, our clients and candidates) that may be affected by an actual or suspected data breach. The Privacy Officer will manage such communications (or delegate to the appropriate person) in consultation with Hudson's General Counsel.

Breach of this policy

Failing to report a data breach may expose Hudson to liability under the privacy and data protection laws. A person who breaches this policy may be subject to disciplinary action, up to and including termination of employment.