ATLANTIC DIGITAL PRIVACY POLICY

Purpose

The Privacy Act 1988 (Privacy Act) is the principal piece of Australian legislation protecting the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information in the public and private sectors. Atlantic Digital takes its obligations under the Privacy Act seriously when handling all corporate and personal information, including customer, vendor and employee information.

Atlantic Digital is committed to providing quality services to our customers. Individuals and our employees and this policy outlines our ongoing obligations in respect of how we manage all Personal Information.

Customer information, including information about our customer's employees and contractors may be collected and stored for bona-fide business purposes throughout the course of a customer's engagement with Atlantic Digital; including during the on-boarding process, during business as usual interactions and, from time to time, through activities such as data migrations.

We have adopted the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth) (the Privacy Act). The APPs govern the way in which we collect, use, disclose, store, secure and dispose of all Personal Information.

By subscribing to, purchasing or using Atlantic Digital services individuals and organisations consent to the collection, transfer, processing, storage, disclosure and other uses of personal information as described in this Privacy Policy. Atlantic Digital will retain private information for as long a personal/customer account is active, or as reasonably useful for commercial purposes or as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

This Privacy Policy applies to the information that we obtain through the provision of Atlantic Digital's own internal systems; services via a devices such as a computer, laptop, tablet or mobile phone or when our customers otherwise interact with Atlantic Digital. Atlantic Digital's services include our websites, support services and the provision of external products or services, for which separate privacy policies can be provided on request.

Sensitive Information

Atlantic Digital does not collect or store any sensitive information as defined in the Privacy Act.

Third Parties

Where reasonable and practicable to do so, we will collect customer/personal information only from organisations/individuals who provide this information freely and directly. However, in some circumstances we may be provided with information by third parties. In such a case we will take reasonable steps to ensure that individuals are made aware of the information provided to us by the third party.

Disclosure of Personal Information

Customer/personal information may be disclosed in a number of circumstances including the following:

- Third parties where customers/individuals consent to the use or disclosure; and
- Where required or authorised by law.

Atlantic Digital will never sell or disclose customer/personal information outside of these requirements.

Security of Personal Information

Customer/personal information is stored in a manner that reasonably protects it from misuse and loss and from unauthorised access, modification or disclosure. Atlantic Digital takes steps to protect the personal information we hold against loss, unauthorised access, use, modification or disclosure, and against other misuse. These steps include password protection and access privileges for accessing our IT systems, securing paper files in locked cabinets, and physical access restrictions.

If a data breach occurs and customer/personal information that we hold is subject to unauthorised loss, use or disclosure, Atlantic Digital will respond in accordance with the Privacy Act.

The Privacy Act requires Atlantic Digital to notify relevant customers/individuals, the Office of the Australian Information Commissioner and any other relevant agencies of any unauthorised access or disclosure of customer/personal information which would be likely to result in serious harm to affected organisations or individuals.

If Atlantic Digital reasonably suspect that there has been such unauthorised access or disclosure, we will carry out an expeditious assessment to determine if it is an 'eligible data breach' and take all reasonable steps to contain the unauthorised access and follow procedures around disclosure of the incident as required by the Australian government. Atlantic Digital will complete our review within 30 days of becoming aware of the potential personal information breach.

When customer/personal information is no longer needed for the purpose for which it was obtained, Atlantic Digital will take reasonable steps to destroy or permanently de-identify such customer/personal information. However, most of the customer/personal information is or will be stored in client files which will be securely kept by Atlantic Digital for a minimum of 7 years.

Access to Customer/Personal Information

Customers/individuals may access the personal information we hold about them and update and/or correct it, subject to certain exceptions. Customers/individuals wishing to access their personal information are required to contact Atlantic Digital in writing to access/update their personal information.

Atlantic Digital will not charge a fee for any access request, but may charge an administrative fee for providing a copy of any customer/personal information.

In order to protect all customer/personal information we may require identification before releasing the requested information.

Maintaining the Quality of Customer/Personal Information

It is an important to us that all customer/personal information is up to date. Atlantic Digital will take reasonable steps to make sure that all customer/personal information is accurate, complete and up-to-date. If a customer/individual finds that the information we have is not up to date or is inaccurate, they can advise Atlantic Digital as soon as practicable so we can update our records and ensure we can continue to provide trustworthy, quality services.

Management of Employee Records

The primary purpose for collecting employee information is to maintain employee records adequately to properly manage employment circumstances, salary and superannuation details. Atlantic Digital will only retain an employee's personal information for as long as is required for this reason, or where the company is otherwise required to retain this information by law.

Atlantic Digital will take reasonable steps to ensure that any personal information collected, is stored in a secure manner, regardless of whether it is collected or stored in electronic or paper format. Atlantic Digital will ensure that such information is protected from unauthorised disclosure and will only share such information for purposes related to the management of each individual employee's circumstances, or where legally required to do so.

Employees may request access, or correction where applicable, to any records regarding their employment, unless this would unreasonably impact on the privacy of others, or breach Atlantic Digital's legislative obligations.

Employee Obligations

Personal information can include information relating to employee's:

- Recruitment, performance, discipline, resignation or termination;
- Terms and conditions of employment;
- Personal contact details;
- Hours of work and remuneration;
- Membership of a trade association or union;
- Leave entitlements; or
- Banking, taxation and superannuation details.

Atlantic Digital may also access or collect any computer, internet, phone or other records or information that has been created or accessed during the course of any employee's employment using company equipment and resources.

Atlantic Digital may collect information relating to any employee's health or personal circumstances, where this is disclosed and relevant to the role, such as where a nominated treating doctor has disclosed restrictions on an employee's ability to perform certain tasks for their safety.

Employees must take their obligations under the Privacy Act seriously. Employees must ensure they handle any employee or client information in accordance with the Privacy Act and do not disclose it unlawfully. This includes ensuring that any personal information encountered during the performance of their duties is kept private and only used for a proper purpose.

Breaches of this policy are taken seriously and disciplinary action, including, but not limited to termination of employment, may be taken for such breaches.

Document Version: February 2018