Pacific Internet Solutions
Privacy policy 28/01/2022

Introduction

Our company Pacific Internet Solutions set itself the goal of achieving the maximum confidence of our clients and contracts. We know that in this new digital era a very important factor for correct access, proper service, reliable communications and transparency, is the management of information and its corresponding privacy.

For this reason, we have created this privacy policy that will agree on the norms, rights and the establishment of clear and precise rules for healthy coexistence in our relationship with our clients.

Our policy that we will proceed to develop below is based on The Privacy Act 1988 (The Privacy Act) since it is the regulation act of the privacy principles drafted for countries such as Australia. With the aforementioned, it is worth saying that in this last act the principles of the Privacy Act 2012 (enhancing privacy protections) are already amended. In addition, our text is also based on the Australian Privacy Principles (APPs) which allows us to better manage the collection, use, and disclosure of information. For example, sets out principles that require APP entities to consider the privacy of personal information (regarding its 13 principles), including ensuring that APP entities manage personal information in an open and transparent way, or sets out principles that deal with the collection of personal information including unsolicited personal information.

This policy will be delivered to you at the time of contracting our information storage and management services, so it is vital for the correct fulfillment of this, that you give your consent and approve our policy, otherwise it would be impossible to improve our service.

On the next pages we will detail the most relevant concepts that we consider in our policy, such as: **The purpose of collecting data, what king of personal information we collect and hold, what type of data is collected, what is done with the collected data, Among other important topics.**

General Definitions

In order to clarify some concepts that can be confusing, and at the same time be frequent in our policy, we will highlight some with their corresponding meaning:

Personal Information: Means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.

Identification Information: Means the individual´s full name or an alias or previous name of the individual or the individual´s date of birth or the individual´s sex or his/her current or last known address.

Identifier of an individual: Is a number, letter or symbol, or a combination of any or all those things, that is used to identify the individual or to verify the identity of the individual, but does not include: The individual name or the individual´s ABN or anything else prescribed by the regulations.

Payment Information: is a statement that the amount of the overdue payment has been paid on that day.

Credit: is a contract, arrangement or understanding under which a payment of a debt owed by one person to another person is deferred or one person incurs a debt to another person and defers the payment of the debt.

Sensitive information: Means information or an opinion about an individual´s racial or ethnic origin or political opinions or membership of a political association; or religious beliefs or philosophical beliefs or membership of a professional or trade association or membership of a trade union or sexual orientation or practices or criminal record that is also personal information, or genetic information about an individual that is not otherwise health information or biometric information that is to be used for the purpose of automated biometric verification or biometric identification or templates.

Data Base Management System (DBMS)

For the sole reason that the information in this policy is clear and transparent, we will detail some aspects of information management that we believe is important for our clients and employees.

A database is an organized collection of information or structured data, which is usually stored electronically in a computer system. Our database software is Oracle with the Autonomous Data base model.

That said, and with all the tools that the system allows us to, for example, automate protection and security, self-repair among many other alternatives that we will detail in this text, it will also give us the possibility to divide the information between our clients and our employees, it is saying these aspects we will treat them differently, we know that the needs are different and we adapt to these differences.

As well as this differentiation, we will also treat confidential and non-confidential data differently, this will give us the possibility of delivering a faster and more effective service.

In this link you can find information and characteristics of our database software.

https://www.oracle.com/mx/autonomous-database/

Privacy Principles in Australia Statements

The 1988 act includes the Australian Privacy Principles (App), as part of its privacy policies. The Apps mentioned are 13, which are divided into 5 parts. Next, we will list the parts with their respective principles and we will also add each statement that we consider meets the expectation of the Pacific Internet Solutions policy.

Part 1- Consideration of personal information privacy: Sets out principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.

1._ App 1: Open and transparent management of personal information
2._ App 2: Anonymity and pseudonymity

Statement

As Pacific Internet Solutions we are committed to following the regulations of the 1988 act and the Australian App privacy principles to better carry out the handling of our clients' Personal Information, whether it is an identity or a natural person, in addition to any case of breach or doubt of our users, we are absolutely committed to facilitating the way to find a prompt solution to the possible discussion. We are determined to deliver the best of services so this policy will be delivered and available on our website www.PacificInternetSolutions.com.au.

With the goal of complying with the 1988 act as a guide, the anonymity rights of individuals will be fulfilled, that is, the obligation of the individual's real name is not necessary and a pseudonym can be used, except that the law or an Australian court requires.

Our database software allows us to divide the information between clients and employees. Our information management has decided that the information of our clients will be updated every end of the month and that of our employees every 2 months. After each update the information will be deleted or kept according to its properties and the time in which the information was collected.

Every 1 year the information will go to a file system where from the following month its deletion will be evaluated. Before moving to the filing system, our clients will be notified of the measures taken.

Part 2- Collection of personal information: Sets out principles that deal with the collection of personal information including unsolicited personal information.

3._ App 3: Collection of solicited personal information
4._ App 4: Dealing with unsolicited personal information
5._ App 5: Notification of the collection of personal information

Statement

The purpose of the collection of information will be to strengthen and improve the service of our service to our clients and entities that request our service. It could be, for example, to: provide required services, provide information on any pending matter or request additional information, effectively speed up legal processes that can serve for a better development of our own internal operation, among others.

We will not collect any information or data that the individual does not want to deliver to us, however this could mean not having the information necessary to deliver the requested service.

The information collected will be solely and exclusively related to us for the purpose that the individual requires.

The information required by our company could be, for example: name, year of birth, telephone numbers, email addresses, credit card data, user names, passwords when requesting access to our services.

Our clients have the right that their information will be stored safely and reliably with methods that we will detail later.

If for any reason we obtain information about you, whether or not you have provided it, or in the event that any external entity or organization, whether under any Australian law or court, requires all or part of your personal information, you have the right and you will be instantly notified when this happens.

For any questions, queries, comments that may appear, do not hesitate to contact us through the communication channels that we have, both by telephone and on social networks.

The method of collecting information on our part will be through formal and established channels, it could be under a survey where we will require your information, or it could be through a meeting that you can establish with us, under the social networks where we have communication channels. Via email where we will have a safe and reliable channel of understanding.

We have a safe and fast chat also on our website, which could quickly and effectively solve any question regarding your information.

Part 3- Dealing with personal information: Sets out principles about how APP entities deal with personal information and government related identifiers. The part includes principles about the use and disclosure of personal information and those identifiers.

6._ App 6: Use or disclosure of personal information
7._ App 7: Direct marketing
8._ App 8: Cross-border disclosure of personal information
9._ App 9: Adoption, use or disclosure of government related identifiers

Statement

As a company created for the connectivity, storage and computing of information, we are committed to the privacy of each of our clients. We know that confidentiality is one of the main concerns of the new digital world, so the information collected will not be used or disclosed for secondary purposes unless our clients consent to it. The information will only be used for the main purpose for which it was collected.

Therefore, it could be used to verify your identity, and to be able to contact you, manage financial aspects such as creating invoices, receipts, debt management, among others.
In addition, to be able to promote and advertise some services that might seem interesting to you, of course there are channels to be able to unsubscribe from this advertising if you so require, we can also review your use of our services to improve them and we will know how and when you use them.

We will not disclose your personal information unless you give us your consent or it is required by Australian law or a court or tribunal both in Australia and abroad, in addition to ensuring that in the case of handling abroad it is in accordance to the PPP Principles Act.

Part 4- Integrity of personal information: Sets out principles about the integrity of personal information. The part includes principles about the quality and security of personal information.

10._ App 10: Quality of personal information
11._ App 11: Security of personal information

Statement

We will maintain all the security mechanisms that we have available so that both confidential and non-confidential personal information is safe, complete, organized and up to date.

In addition, our encryption systems will do everything possible so that its privacy is intact and with the prohibition of any external access other than that of our own clients.

However, we know that connectivity is not 100% secure, so there could be a case of leakage, but we will make sure to do everything in our power so that this does not happen.

It should be noted that we will keep your information only as long as you require it or is necessary to deliver our service no later than 3 years, since after your consent it will be archived on special servers where they can be prepared for elimination.

To confirm reliable secure access and authentication, we have two security protocols: ssl and https. That will serve as the basis of reliability for both us and our users towards our information database.

Ssl (Secure Socket Layer) guarantee the integrity of any sensitive data exchanged. This will prevent hackers and malicious software from reading and changing any transferred data, including sensitive data such as credit card numbers and documents.

This security protocol works through encryption algorithms, encoding the data in transit.

With ssl we will avoid phishing and other possible attacks since with this technology the probability of this type of trap happening is almost nil.

For online payments, ssl is essential, so our users can make their transactions safely.

We also have the Https protocol that encrypts the data exchanged to keep it safe from prying eyes. This means that, when a user is browsing a website, no one can "listen" to their conversations, track their activities through the different pages or steal information, and that the authentication that demonstrates that users communicate with the intended website. It provides protection against man-in-the-middle attacks and builds user trust, ultimately creating other business benefits.

Oracle Autonomous Database automatically backs up the database for us. The retention period for backups is 60 days. It can restore and recover database to any point-in-time in this retention period. We do not have to do any manual backups for the database as Autonomous Database do it automatically.

In order for the access and security of the information you provide us to be even more secure, we will have a dedicated server located in a duly encrypted office so that only authorized personnel can access it and at the same time the dedicated server is completely dedicated to this task without its resources being dedicated to another function.

Part 5- Access to, and correction of, personal information: Sets out principles that deal with requests for access to, and the correction of, personal information.

12._ App 12: Access to personal information
13._ App 13: Correction of personal information

Statement

Our clients will have access to their information when they require it in the way that both parties agree.

We will reserve access to the information or study the case in the circumstance in which it could be harmful to another individual or is restricted by any government law or could be used to violate the privacy of another entity.

To access personal information, please write to our email PacificInterntet@Solutions.com and we will have a secure, reliable and available registry.

If for any reason our clients think that the personal information is incorrect, incomplete or out of date, please contact us via email PacificInternet@Solutions.com in order to find the problem and solve it as quickly as possible. If the correction of the information is rejected, we will let you know the reason by this same means.

How is sensitive data in backups protected?

Database Security

The complexities of database security and some practices, policies, and technologies, will protect the confidentiality, integrity, and availability of the data.

What is database security?

Database security refers to the range of tools, controls, and measures designed to establish and preserve database confidentiality, integrity, and availability.

Database security must address and protect the following:

_ The data in the database
_The database management system (DBMS)
_Any associated applications
_ The physical database server and/or the virtual database server and the underlying hardware.
_The computing and/or network infrastructure used to access the database

Database security is a complex and challenging endeavor that involves all aspects of information security technologies and practices. It is also naturally at odds with database usability. The more accessible and usable the database, the more vulnerable it is to security threats; the more invulnerable the database is to threats, the more difficult it is to access and use.

Attacks on backups

Organizations that fail to protect backup data with the same stringent controls used to protect the database itself can be vulnerable to attacks on backups.

These threats are exacerbated by the following:

_**Growing data volumes:** Data capture, storage, and processing continues to grow exponentially across nearly all organizations. Any data security tools or practices need to be highly scalable to meet near and distant future needs.

_**Infrastructure sprawl:** Network environments are becoming increasingly complex, particularly as businesses move workloads to multicloud or hybrid cloud architectures, making the choice, deployment, and management of security solutions ever more challenging.

_**Increasingly stringent regulatory requirements:** The worldwide regulatory compliance landscape continues to grow in complexity, making adhering to all mandates more difficult.

_ **Cybersecurity skills shortage:** Experts predict there may be as many as 8 million unfilled cybersecurity positions by 2022

Pacific Internet Solutions Best Practices

Because databases are nearly always network-accessible, any security threat to any component within or portion of the network infrastructure is also a threat to the database, and any attack impacting a user´s device or workstation can threaten the database. Thus, database security must extend far beyond the confines of the database alone.

When evaluating database security, the environment to decide on the team´s top priorities, we consider each of the following areas:

_**Physical security:** Whether the database server is on-premise or is a cloud, it must be located within a secure, climate-controlled environment.

_**Administrative and network access controls:** The practical minimum number of users should have access to the database, and their permissions should be restricted to the minimum levels necessary for them to do their jobs. Likewise, network access should be limited to the minimum level of permissions necessary.

_ **End user account/device security:** Always be aware of who is accessing the database and when and how the data is being used. Data monitoring solutions can alert if data activities are unusual or appear risky. All user devices connecting to the network housing the database should be physically secure (in the hands of the right user only) and subject to security controls at all times.

_**Encryption:** All data- including data in the database, and credential data – should be protected with best-in-class encryption while at rest and in transit. All encryption keys should be handled in accordance with best-practice guidelines.

_Database software security: Always use the latest version of your database management software, and apply all patches as soon as they are issued.

_ Application/web server security: Any application or web server that interacts with the database can be a channel for attack and should be subject to ongoing security testing and best practice management.

_Backup security: All backups, copies, or images of the database must be subject to the same (or equally stringent) security controls as the database itself.

_Auditing: Records all logins to the database server and operating system, and log all operations performed on sensitive data as well. Database security standard audits should be performed regularly.

Data protection tools and platforms

Today, a wide array of vendors offers data protection tools and platforms. The full-scale solution will include all of the following capabilities.

_Discovery: A tool that can scan for and classify vulnerabilities across all the databases – whether they are hosted in the cloud or on-premise – and offer recommendations for recommendations for remediating any vulnerabilities identified. Discovery capabilities are often required to conform to regulatory compliance mandates.

_Data activity monitoring: The solution should be able to monitor and audit all data activities across all databases, regardless of whether the deployment is on-premises, in the cloud, or in a container. It should alert to suspicious activities in real-time so that can respond to threats more quickly. We want a solution that can enforce rules, policies, and separation of duties and that offers visibility into the status of the data through a comprehensive and unified user interface. It must generate the reports that will be needed to meet compliance requirements.

_Encryption and tokenization capabilities: In case of a breach, encryption offers a final line of defense against compromise. The tool will include flexible encryption capabilities that can safeguard data in on-premise, cloud hybrid, or multicloud environment. The tool will have file, volume, and application encryption capabilities that conform to the industry´s compliance requirements, which may demand tokenization (data masking) or advanced security key management capabilities.

_**Data security optimization and risk analysis:** A tool that can generate contextual insights by combining data security information with advanced analytics will enable to accomplish optimization, risk analysis, and reporting with ease. The tool can retain and synthesize large quantities of historical and recent data about the status and security of the database, and look for one that offers data exploration, auditing, and reporting capabilities through a comprehensive bur user-friendly self-service dashboard.

The Solution: Database security and IBM cloud

IBM-managed cloud databases feature native security capabilities powered by IBM Cloud Security, including built-in identity and access management, visibility, intelligence, and data protection capabilities. With and IBM- managed cloud database, PIS can rest easy knowing that the database is hosted in an inherently secure environment.

IBM also offers the IBM Security Guardium smarter data protection platform, which incorporates data discovery, monitoring, encryption and tokenization, and security optimization and risk analysis capabilities for all databases, data warehouses, file shares, and big data platforms, whether they are hosted on-premises, in the cloud, or in hybrid environments.

In addition, offers managed Data Security Services of Cloud, which includes data discovery and classification, data activity monitoring, and encryption and key management capabilities to protect the data against internal and external threats through a streamlined risk mitigation approach.

The aforementioned solution will be the data management protection system, in our PIS information management system.

For any questions or comments, you may have regarding this policy or the procedures described in it, please do not hesitate to contact us. As Pacific Internet Solutions we are excited to be able to clarify your doubts as soon as possible, our staff will be available for you.

Below are the contact methods of our Data center:

www.PacificInternetSolutions.com
Contact: 048975216
PacificInternet@Solutions.com
@PacificInternetSolutions
#SafeDataSolutions

2/246 Varsity Parade, Varsity Lakes QLD 4227