

Uptown ICT

&

Privacy Policies

Version: V1.5



Contents

[Privacy Policy 3](#_Toc113365104)

[Policy Document number: 3](#_Toc113365105)

[Current until: 3](#_Toc113365106)

[Background 3](#_Toc113365107)

[Purpose 3](#_Toc113365108)

[Policy Statement 3](#_Toc113365109)

[Classification of Data 4](#_Toc113365110)

[Encryption 6](#_Toc113365111)

[Hash Functions 6](#_Toc113365112)

[Data Access 6](#_Toc113365113)

[Data Backup 6](#_Toc113365114)

[Data Deletion 7](#_Toc113365115)

[Privacy Impact Statement 7](#_Toc113365116)

[International Standards 7](#_Toc113365117)

[Online Account Audits/Governance 7](#_Toc113365118)

[Policy Compliance 8](#_Toc113365119)

[Compliance Measurement 8](#_Toc113365120)

[Exceptions 8](#_Toc113365121)

[Non-Compliance 8](#_Toc113365122)

[Definitions and Terms 11](#_Toc113365123)

[Revision History 11](#_Toc113365124)

# Privacy Policy

Policy Document number: V2

Current until: 30 December 2023

## **1.1 Background**

This policy is based on Privacy Act of 1988, Australian Government, Office of the Australian Information Commissioner

https://www.oaic.gov.au/privacy/the-privacy-act/

And when dealing with state government entities, Information Privacy Act 2009 Queensland Government, public sector environment

http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/qld/consol\_act/ipa2009231/

## **1.2 Purpose**

The purpose of this policy is to set out guidelines to be followed by all staff in the collection and handling of client information for Uptown

## **1.3 Policy Statement**

The purpose of this policy is to provide guidance on how Uptown Marketing classifies, labels, and restricts access to, sensitive data. How Uptown Marketing and employees’ store, transfer and ensure data integrity of sensitive data.

**2. Personal Information**

Ensuring and maintaining the integrity, confidentiality, security, and availability of information that is collected and how personal information will be kept safe and secure from unauthorised access, modification or disclosure, misuse, and loss:

 • Regularly monitoring information handling practices to ensure they are secure.

• Password protection.

• Backups.

• Offsite storage.

• Encryption.

• Firewalls.

• Cookie removers.

• Anti-virus scanners.

• Checking that all personal information has been removed from electronic devices before they are sold or destroyed.

• Deleting out-of-date customer records and how this will be done i.e.:

o Shred, pulp or destroy paper records.

o Dispose of files in security bins.

o Delete electronic records or files securely so that they cannot be retrieved.

**3. Classification of Data**

With personal information you should consider how you will protect personal information during the stages of its life cycle, as specified by the Australian Government Office of the Australian Information Commissioner website.

Personal information security throughout the life cycle involves:

* Considering whether it is actually necessary to collect and hold personal information in order to carry out your functions or activities.
* Planning how personal information will be handled by embedding privacy protections into the design of information handling practices.
* Assessing the risks associated with the collection of the personal information due to a new act, practice, change to an existing project or as part of business as usual.
* Taking appropriate steps and putting into place strategies to protect personal information that you hold.
* Destruction or de-identification of the personal information when it is no longer needed.

All Uptown Marketing data transmitted, received or stored is required to be identified and classified as Unofficial, Official or Official: Sensitive.

All Unofficial data, documents and/or removable drives that hold this data do not require to be labelled or have access restricted. Unofficial data does not require to have storage location tracked.

All Official data, documents and/or removable drives that hold this data require to be labelled with a Yellow label but does not require restricted access. Official data requires tracking of current storage location.

All Official: Sensitive data documents and/or removable drives that hold this data require to be labelled with a Red label and requires restricted access to only authorised employees. Official: Sensitive data requires tracking of current storage location and audit trail of movement throughout the organisation.

|  |  |  |
| --- | --- | --- |
| **Protective marking** | **Business impact level** | **Compromise of information confidentiality would be expected to cause:** |
| **UNOFFICIAL** | No business impact | No damage. This information does not form part of official duty. |
| **OFFICIAL** | 1 Low business impact | No or insignificant damage. This is the majority of routine information.  Example: Job Advertisement |
| **OFFICIAL: Sensitive** | 2 Medium business impact | Limited damage to an individual, organisation or government generally if compromised. Falls under the Privacy Act 1988 and Australian Privacy Principals. Example: Employee and Customer PII data |

**4. Storage/sharing and control**

**4.1 Encryption**

The reason for file and hard disk encryption is to safeguard data stored on a device such as a computer, or any type of network storage device. Organisations, including micro and small businesses, which collect personal or sensitive information must secure that data. The organization can suffer fines for individual and the organisation itself if breaches occur.

Full Disk Encryption is required on all devices and must use XTS-AES 128-bit encryption.

Sensitive folders must have XTS-AES 128-bit encryption enabled with authorized users provided with key.

All removable devices that hold Official or Official: Sensitive data must be encrypted with XTS-AES 128-bit encryption.

**4.2** **Hash Functions**

Prior to storing sensitive data files, a SHA-512 has must be run on the completed file. This must be run after the transfer and the hashing outputs compared to ensure data integrity.

**4.3 Data Access**

Only authorised users have access to Official: Sensitive data and the folders that contain this data.

Object auditing must be enabled and logged to ensure data integrity of sensitive data and track user access and modifications to the sensitive data.

**4.4 Data Backup**

All data backups that exceed 10Gigabytes are to be performed during off peak hours.

All off-site electronic data backups are to be stored through the use of a cloud provider over a SSL connection or VPN. It can also be stored in a secure location through the use of a secure transport company on an encrypted USB or full disk encrypted Hard-Disk Drive.

All on-site electronic backups are to be stored on a secure server that has full disk encryption and is only sent and retrieved through secure software protocols.

All hardcopy backups of sensitive data are to be securely stored in a locked safe and/or filing cabinet.

Only authorized personnel are to have access to the backup server, media or cloud provider.

**4.5 Data Deletion**

All data must be deleted using the Eraser software.

Any removable devices and hard disk drives must be physical destroyed.

All documents must be shredded using a crosscut shredder or incineration.

**5. Privacy Impact Statement**

Privacy Impact Statement is required to be completed to ensure privacy standards are being met and any risks to data privacy are identified and managed.

**6. International Standards**

Uptown Marking may hold European citizen client data and as such requires to be GDPR compliant. A completed GDPR Data Protection and Compliance Checklist is required and must be re-checked with any changes to this policy or procedures.

**6. Online Account Audits/Governance**

Uptown Marketing requires all employees to uphold the below standards for all online accounts to reduce the risk of fraud, identity theft and social engineering practices. There is a pre-prepared Audit checklist to assist in this process.

Delete all unused accounts to reduce information footprint.

Remove any sensitive personal and/or organisational information in all profiles even if that profile is unused.

Create multiple strong passwords across personal and organisation accounts/profiles.

Configure and use 2FA across all accounts where available.

Adjust privacy settings across all Social Media accounts to allow access to only authorised individuals and restrict social engineering threats from attackers.

Adjust spam filter settings across all Email accounts to ensure spam/phishing emails are scanned and filtered correctly.

Adjust privacy and security settings across all Banking accounts to ensure a reduction in security threats.

Adjust privacy and security settings across all Internet Browsing Software to restrict location tracking, ensure all popups are blocked by default and increase the default securing settings to high.

Adjust privacy and security settings across all Mobile Devices and Applications to remove all sensitive information from being leaked from the device or applications.

**7. 1 Policy Compliance**

**Compliance Measurement**

The IT Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

**7.2 Exceptions**

Any exception to the policy must be approved by the IT team in advance.

**7.3 Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**8. Documentation Policy**

All Uptown IT official documentation will be recorded in the Uptown IT Document Register. Any new documents created must be entered into the register. Any revisions to existing documents must be noted in the document register.

Version control must be used on all Uptown IT documentation. Latest versions must be used for all new documentation. All existing documentation must be transferred to the latest template version during periodic reviews.

A document register must be created for all clients. All documents relating to that client must be entered into the register. Any revisions to existing documents must be noted in the document register.

All work carried out by Uptown IT must be fully documented. Templates are available for a variety of documentation types. Where a template is not available, documentation must be created on an Uptown IT letter head and must be clear and concise. All possible variables must be documented with settings and configuration details.

**8.1 Naming Conventions**

Naming conventions must be fully documented for each system created by Uptown IT employees. If abbreviations or codes are used in the naming conventions, a full list of abbreviations and their meaning must be included in the naming conventions documentation.

Computers

All computers will be named in 4 sections

• Section 1 – abbreviated client name

• Section 2 – device type

• Section 3 – device location

• Section 4 – device number

**8.2 Folders**

Folders will be named in 2 sections

• Section 1 – abbreviated client name

• Section 2 – abbreviated folder contents

**8.3 Computer Domains**

Where the client has a registered domain name, that name, or a sub domain of that name is to be used.

Where the client does not have a registered domain name, a registered domain name may be purchased. If the client does not wish to purchase a domain name, a suitable name is to be used, incorporating the client’s name or abbreviation of the client’s name.

Security Groups

Security groups will be named with a meaningful name that gives an indication of the function of the group members.

All group names will start with an uppercase letter and have no gaps. Where multiple words are used in the name, the first letter of each new name will be capitalised.

Users

User logon names will be, user’s full last name and first initial of first name, all one word, all lower case and a number starting at 1, and incrementing by one for each additional user with the same username.

**9. Network Addressing**

Networks will use IPv4 addressing. All networks will use the 192.168.0.0 network with appropriate subnet mask to unsure sufficient addresses are available for all devices and future growth.

Where multiple subnets are required, the 192.168.0.0 network will be used and sub-netted as required.

Sharing and managing of sensitive data on network shall only be permitted to authorised staff within the application scope or project.

Network administrator to monitor all activities of sensitive information and report any issues that occur.

An authorised person having access to network on should have the knowledge of:

• Principles of the Privacy Act 1988

• Understand data protection and encryption

• How to identify changes in systems and programs that indicate malicious intrusion

Access permissions:

• Strong password policy

• Two-factor authentication

Encryption of data

Hashing for data integrity

**10. Media storage and labelling**

Media is classified to the highest sensitivity or classification of data it stores.

a) Storage

Storage of media not in use for a scheduled backup shall be located in a fireproof safe with at least a 2-hour fire rating. Alternatively, media can be transported off-site each night by a designated staff member. Off-site location needs to be secure.

b) Labelling

Labelling media helps personnel to identify its sensitivity or classification and ensure that appropriate measures are applied to its storage, handling and use.

Labelling of media must be in accordance with the backup schedule and labelled with the correct sequence

Media is to be labelled with protective markings reflecting its sensitivity or classification. Therefore, media containing official data will be labelled with a Yellow label. Media containing sensitive data will require a Red label and restricted access (only authorised employees).

**Related Standards, Policies and Processes**

<https://www.legislation.gov.au/Details/C2021C00139>

<https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx>

<https://gdpr.eu/checklist/>

<https://www.nist.gov/itl/smallbusinesscyber/securing-data-devices>

<https://www.business.qld.gov.au/running-business/protecting-business/risk-management/protecting-data/policies-procedures>

<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment>

**Definitions and Terms**

Encryption: Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used

Advanced Encryption Standard (AES): An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.

Hash Functions: (cryptographic) hash functions are used to generate a one way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHA1.

Software: Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| April 2021 | George Brown | Created |
|  |  |  |