**Security Policy**

Created by

**UPTOWN IT**

**PROJECT REFERENCE:**

**DATE:**

Contents

[Revision History 2](#_Toc117590287)

[1. Purpose 3](#_Toc117590288)

[2. Scope 3](#_Toc117590289)

[3. Policy 3](#_Toc117590290)

[3.1 Classification of Data 3](#_Toc117590291)

[4.2 Encryption 4](#_Toc117590292)

[4.3 Hash Functions 4](#_Toc117590293)

[4.4 Data Access 4](#_Toc117590294)

[4.5 Data Backup 4](#_Toc117590295)

[4.6 Data Deletion 5](#_Toc117590296)

[4.7 Privacy Impact Statement 5](#_Toc117590297)

[4.8 International Standards 5](#_Toc117590298)

[4.9 Online Account Audits 5](#_Toc117590299)

[4.10 Cyber Awareness 5](#_Toc117590300)

[4.11 Acceptable Use of Social Media 6](#_Toc117590301)

[4.12 Bring your own device 6](#_Toc117590302)

[4. Policy Compliance 6](#_Toc117590303)

[5.1 Compliance Measurement 6](#_Toc117590304)

[5.2 Exceptions 6](#_Toc117590305)

[5.3 Non-Compliance 6](#_Toc117590306)

[5. Related Standards, Policies and Processes 7](#_Toc117590307)

[6. Definitions and Terms 7](#_Toc117590308)

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| DATE | RESPONSIBLE | SUMMARY of CHANGE | APPROVED BY |
| 3rd Oct 2022 | George Brown | Created | Manager |
|  |  |  |  |

# Purpose

The purpose of this policy is to provide guidance on how MidTown IT classifies, labels, and restricts access to, sensitive data. How MidTown IT and employees’ store, transfer and ensure data integrity of sensitive data. It will also provide guidance on adhering to onshore and offshore data protection standards and legislation.

# Scope

This policy applies to all MidTown IT employees and affiliates.

# Policy

## Classification of Data

All MidTown IT 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 labeled 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 must be labeled with a Yellow label but do not require restricted access. Official data requires tracking of the current storage location

All Official-Sensitive data documents and/or removable drives that hold this data require to be labeled with a Red label and require restricted access to only authorised employees. Official-Sensitive data requires tracking the 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 |

## 4.2 Encryption

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.

## 4.3 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.

## 4.4 Data Access

Only authorized 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.

## 4.5 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 the secure server that has full disk encryption and only sent and retrieved through secure software protocols.

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

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

## 4.6 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

## 4.7 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.

## 4.8 International Standards

MidTown IT 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.

## 4.9 Online Account Audits

MidTown IT 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

## 4.10 Cyber Awareness

MidTown IT requires all employees to complete the Cyber Security Awareness questionnaire upon employment and when requested by the senior leadership team.

Upon completing this questionnaire, you will be provided with a score out of 100 and given a rating as described below. This score will be stored and used as information for the organization-wide Cyber Security awareness standard.

MidTown IT’s goal is to have an average organizational standard of >75%

Questionnaire ratings are scored as Low, Medium and High, as the table below.

|  |  |
| --- | --- |
| 0-40 | Low |
| 41-74 | Medium |
| 75-100 | High |

## 4.11 Acceptable Use of Social Media

Limited and occasional use of MidTown IT systems to engage in Social Media is acceptable, if it is done in a professional and responsible manner, is not detrimental to MidTown IT best interests, and does not interfere with an employee's regular work duties. Social Media use from MidTown IT systems is also subject to monitoring.

MidTown IT Confidential Information policy also applies to Social Media. As such, Employees are prohibited from revealing any MidTown IT confidential or proprietary information.

Employees must follow all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, MidTown IT trademarks, logos and any other MidTown IT intellectual property may also not be used in connection with any personal Social Media activity.

## 4.12 Bring your own device

MidTown IT employees are permitted to bring their own devices to the workplace.

Any devices owned by MidTown IT employees are subject to the sections in this policy.

# Policy Compliance

## 5.1 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.

## 5.2 Exceptions

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

## 5.3 Non-Compliance

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

# Related Standards, Policies and Processes

Related standards, policies and processes can be accessed visiting the following links:

<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

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.