Data Storage Policy

Title: Morgan Maxwell Design Data Storage Policy	
Department: IT	**Version:** 001
Approved by: Jing Chan	**Approval Date: 12/07/2022**
Effective Date: 19/07/2022	**Last Updated:**
Author: Peta Paul	

Scope

This policy applies to Morgan Maxwell Design employees, contractors, consultants, temporary workers and all other individuals storing, using or accessing Morgan Maxwell Design data and information, whether in electronic or hard copy formats.

This policy applies to data storage activities that are on-premises and remotely managed using cloud-based or company-managed storage technology. Data can include all kinds of information, including but not limited to the following:

- client's credit card details
- clients, staff and suppliers' personal information
- financial records.

Responsibility

The Morgan Maxwell Design IT department is responsible for maintaining and updating this policy with the approval of the chief information officer or chief technology officer.

Objectives

The objective of this policy is to define how data – both electronic and hard-copy – will be stored in such a way as to protect it and, ensure its security, availability and protect the privacy of individuals in accordance with established data management policy and compliance with applicable laws, standards and good practice.

Purpose

Morgan Maxwell Design's purpose for data storage is to ensure that all data and information – in electronic or hard-copy form – needed by Morgan Maxwell Design in the performance of its work are stored in a secure repository when not in current use or when archived for future use, such that they are available when needed, are accessible and usable by Morgan Maxwell Design staff, and are maintained in secure, protected environments until they are retrieved for use, archived or destroyed.

The focus of data storage management is to meet the legal requirements for record retention and privacy protection, optimise the use of space, minimise the cost of record retention, and destroy outdated records.

Policy

Morgan Maxwell Design requires that its data and information, whether in electronic or hard-copy formats, are stored securely and managed so that the company:

1. Meets legal standards for data storage, retrieval and protection
2. Establishes procedures for data storage activities, delivers them to all employees, provides training on the policy as part of the new employee onboarding, provides refresher training as needed, and reviews and updates the procedures as needed
3. Protects the data privacy of employees, customers and others as required by law
4. Optimises the use of primary data storage facilities to facilitate the timely and secure retrieval of data from storage when needed
5. Establishes rules for the use of employee-owned storage devices and monitors that usage
6. Addresses security issues associated with data storage on company-owned facilities and third-party managed storage services, as well as employee-owned storage devices, to minimise the potential for unauthorised access to company data and information
7. Plans for and budgets for data storage technology, whether on-site or remote
8. Regularly reviews and adjusts its data storage facilities, both on-site and remote, to promptly accommodate changes in storage requirements

Morgan Maxwell Design may designate an employee as a data storage manager; this employee will most likely be part of the IT department.

Morgan Maxwell Design departments that generate data and information are responsible for establishing appropriate data storage requirements in coordination with the Morgan Maxwell Design data storage manager. Each department's administrative manager or designee must:

1. Be familiar with Morgan Maxwell Design's data storage policy
2. Develop the department's and/or office's data storage requirements consistent with this policy
3. Educate staff within the department so they understand data storage practices
4. Define storage requirements for confidential data and information

Confidentiality Requirement

Some Morgan Maxwell Design data and information may contain nonpublic, confidential data. Such data and information should be stored per Morgan Maxwell Design's privacy and security policies.

Electronically Stored Information

Morgan Maxwell Design depends on the use and availability of electronically stored information (ESI). The ease with which ESI may be created, the technology where ESI may be stored, and rules regarding the use of ESI in litigation all require that Morgan Maxwell Design manages its data storage activities efficiently and consistent with its legal obligations. Accordingly, all departments must include ESI in developing their data storage requirements.

Non-Electronic Information Storage

Morgan Maxwell Design stores important hard-copy documents in secure, fire-protected storage containers located on-site or in secure remote storage facilities. The point at which such information is to be placed into storage and the type of storage to be used is determined by the document's user(s) in collaboration with the data storage manager and/or records manager.

Disposal and Destruction of Stored Data and Information

Where records have been identified for destruction, they should be disposed of appropriately. All information must be reviewed before destruction to determine whether there are particular factors that mean destruction should be delayed, such as complaints or grievances. All paper records containing personal or sensitive policy information should be shredded before disposal. All electronic information must be deleted.

Payroll Records					
Ref	File Description	Data Protection issue	Retention period	Action at the end of the life of the record	Destruction Date
1.1.1	Wages and Salaries	Yes	7 years	Secure disposal	Current year + 6 years
1.1.2	Workers Compensation Claims	Yes	7 years	Secure disposal	Current year + 6 years
1.1.3	Superannuation Fund information	Yes	7 years	Secure disposal	Current year + 6 years

Financial Records					
Ref	File Description	Data Protection issue	Retention period	Action at the end of the life of the record	Destruction Date
2.1.1	Annual Accounts	No	7 years	Secure Disposal	Current year + 6 years
2.1.2	Records relating to the collection and banking of monies	No	7 years	Secure disposal	Current year + 6 years
2.1.3	All records relating to the creation and management of budgets, including the Annual Budget	No	Life of budget + 3 years	Secure disposal	Life of budget + 3 years
2.1.4	Invoices, receipts, order books and requisitions, delivery notices	No	7 years	Secure disposal	Current year + 6 years
2.1.5	Records relating to the identification and collection of debt	No	7 years	Secure disposal	Current year + 6 years

Morgan Maxwell Design maintains a database of records that have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least:

- File reference (or another unique identifier)
- File title/description
- Number of files
- Name of the authorising officer
- Date destroyed or deleted from the system
- Person(s) who undertook destruction.

Enforcement

Morgan Maxwell Design employees who do not comply with this policy and the procedures that may be developed from it are subject to possible disciplinary measures, including termination of employment as determined by Morgan Maxwell Design senior management, department leadership, chief information officer and/or human resources departments.

Management Review

Morgan Maxwell Design executives will review and update policies annually or more frequently when changes are authorised. As changes to Morgan Maxwell Design policies are indicated in the course of business, Morgan Maxwell Design management may launch a change management initiative to change them. All Morgan Maxwell Design policies will be available for review in the course of scheduled audits.

Legislation

The legislation applicable to this policy is:

- The Privacy Act
- Information Privacy Act 2014 (Australian Capital Territory)
- Information Act 2002 (Northern Territory)
- Privacy and Personal Information Protection Act 1998 (New South Wales)
- Information Privacy Act 2009 (Queensland)
- Personal Information Protection Act 2004 (Tasmania)
- Privacy and Data Protection Act 2014 (Victoria)
- Corporations Act
- Australian Consumer Law (ACL)

Password Protection Policy

Title: Morgan Maxwell Design Password Protection Policy	
Department: IT	**Version:** 001
Approved by: Jing Chan	**Approval Date: 15/07/2022**
Effective Date: 28/07/2022	**Last Updated:**
Author: Peta Paul	

Overview

Passwords are an integral aspect of our computer security program. Passwords are the front line of protection for user accounts. A poorly chosen password may result in the compromise of critical Morgan Maxwell Design resources. As such, all Morgan Maxwell Design staff and outside contractors and vendors with access to our systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

This policy aims to establish a standard for creating strong passwords, protecting those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account or any form of access that supports or requires a password on any Morgan Maxwell Design system.

Policy

IT Support Professionals

All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed every 90 days. All systems administrative-level passwords for production environments must be part of an ITSS-administered global password management database.

User accounts with system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user. Where SNMP (system network management protocol) is used, the community strings must be defined as something other than the standard defaults of "public," "private", and "system". They must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv3).

General Users

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every 90 days. Passwords must not be included in email messages or other forms of electronic communication. Passwords must be at least eight (8) characters in length.

All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

General password construction guidelines are used for various purposes at Morgan Maxwell Design, i.e. user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins). Everyone must be aware of how to select strong passwords.

Poor/ weak passwords have the following characteristics:

- The password can be found in a dictionary (English or foreign)
- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, computer terms and names, commands, sites, companies, hardware, software, birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. Any of the above spelled backwards. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or phrase. For example, the phrase might be: "This May Be One Way To Remember", and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password protection standards:

- Change passwords at least once every 90 days.
- Do not write down passwords
- Do not store passwords online without encryption.
- Do not use the same password for Morgan Maxwell Design accounts as for other non-Morgan Maxwell Design access (e.g., personal ISP account, online banking, email, benefits, etc.).

- Do not share Morgan Maxwell Design passwords with anyone, including administrative assistants or secretaries. All passwords must be treated as sensitive, confidential Morgan Maxwell Design information.
- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Don't use the "Remember Password" feature of applications (e.g., Groupwise, Instant Messenger, Internet Explorer, Mozilla).
- If someone demands a password, refer them to this document or have them call the IT Service Desk.
- If an account or password is suspected to have been compromised, report the incident to IT security and change all passwords.
- Password cracking or guessing may be performed on a periodic or random basis by security personnel. If a password is guessed or cracked during one of these scans, the incident will be documented, and the user will be required to change their password.

Accounts Receivable Setup and Invoice Process

A card for each customer must be established in MYOB. This card must contain postal and street addresses, phone numbers and contacts name, email addresses, ABN, and credit limits.

Under the Privacy Act 1988, details must be accurate, kept securely and not given to any person without the customer's consent.

Account customers must complete a credit application, and at least one (1) of the references must be contacted before credit is given.

All account sales are entered into the accounting system at the time of sale. A tax invoice meeting legislation requirements is printed and included with the goods.

All invoices are due 14 days from the invoice date.

Customers are requested to email a remittance if payment is made by electronic funds transfer. These payments must be entered into the accounting system as soon as possible.

Our preferred payment method for account customers is direct deposit into our bank account. Cheques are only accepted from long-term customers and with prior approval. Upon receipt of the cheque, all information must be checked, including the date, the cheque amount, and the cheque is signed.

Accounts Payable Setup and Billing Process

A card for each supplier must be established in MYOB. This card must contain postal and street addresses, phone numbers and contacts, email address, company ABN, bank account details and the suppliers' credit terms.

The expense account to track Purchases will be 5-0100.

Upon receipt of the goods, the goods and tax invoice must be checked against the purchase order to check that the correct goods have been received and the correct amount charged. The store manager authorises the validity of the invoice received. Any discrepancies are followed up immediately.

This tax invoice is recorded in the accounting system, and all accounts are paid within the credit terms. If a part payment of a supplier invoice is necessary, this is made in MYOB against the outstanding amount.

When stock is damaged, not delivered, or there is an error on the supplier invoice, a credit note must be requested from the supplier and entered into MYOB.

A remittance advice is sent to the supplier advising them of the payment amount and the date the payment is made.

Every two (2) weeks, an accounts payable report and a copy of the bank register for the last two (2) weeks are generated to maintain optimal cash flow. Payment of bills is authorised by the Finance Manager from this report, considering the bank account balance and any periodic payments due, such as loan payments (found in recurring transactions).

Payment terms for bills have been negotiated with individual suppliers.

The preferred payment method is EFT into the supplier's nominated bank account.