

Classification of Sensitive Data

1. Purpose

- 1.1. MCS Civil Pty Ltd (MCS) is committed to a high level of security standards to protect our organization from intrusion and data breach. We want to ensure our systems are secured from unauthorized access, so our data and our customers data is safe and secure.
- 1.2. The purpose of this policy is to provide guidance to staff on workstation configuration.

2. Commencement of Policy

- 2.1. This policy will commence 1/07/2024.

3. Application of the Policy and Responsibilities

- 3.1. This policy applies to:
 - 3.1.1. all employees of MCS Civil Pty Ltd (MCS) (whether full-time, part-time or casual) and all persons performing work at the direction of, or on behalf of these entities (for example contractors, subcontractors, agents, consultants, temporary staff and 'workers' as otherwise referred to as 'workplace participants').
 - 3.1.2. all workplaces and to other places where workplace participants may be working or representing MCS Civil Pty Ltd (MCS), for example, when conducting an event (collectively referred to as 'workplace').

4. Definition "Sensitive Data"

- 4.1. Sensitive Data or Sensitive Information is a type of personal information and includes information about the individuals
 - 4.1.1. Health
 - 4.1.2. Racial or Ethnic Origin
 - 4.1.3. Political Opinions
 - 4.1.4. Membership of a political association, professional or trade association or trade union
 - 4.1.5. Religious beliefs or affiliations
 - 4.1.6. Philosophical beliefs
 - 4.1.7. Sexual Orientation or practices
 - 4.1.8. Criminal record
 - 4.1.9. Biometric information

5. Definition "PII" – Personally Identifiable Information

- 5.1. Personally identifiable information is any data that could potential identify a specific individual.
 - 5.1.1. The following are some but not ALL examples of PII
 - 5.1.2. Credit Card
 - 5.1.3. Drivers License
 - 5.1.4. Date of Birth
 - 5.1.5. Address
 - 5.1.6. Proof of Age Card

- 5.1.7. Tax File Information
- 5.1.8. Employee Record
- 5.1.9. Credit Information
- 5.1.10. Signature
- 5.1.11. Email Address
- 5.1.12. Telephone or Mobile Numbers
- 5.1.13. Business or Personal Loan information
- 5.1.14. Work Contract Details

6. MCS Civil Pty Ltd (MCS) Sensitive Data

6.1. MCS Civil Pty Ltd (MCS) has a lot of Sensitive information, not just on customers, but on the MCS Civil Pty Ltd (MCS) itself. The following (but not limited to) is what constitutes sensitive MCS Civil Pty Ltd (MCS) data.

- 6.1.1. Any customer information
- 6.1.2. Any Transactional or Operational records. For eg.
 - All our Emails
 - Accounting Data
- 6.1.3. Any data on our Server
- 6.1.4. Any employee information
- 6.1.5. Information Security or Computer Security
- 6.1.6. Physical Security information
- 6.1.7. Financial Information
- 6.1.8. Processes, policies, procedures or internal documentation

7. Data Breach

- 7.1. Definition: A Data breach is a security incident in which sensitive or PII data is copied, transmitted, viewed, stolen or used by an individual who is not authorized to do so.
- 7.2. Frequently observed data breach methods include but are not limited to the following.
 - 7.3. Unintended Disclosure – Through mistakes or negligence, sensitive data is exposed. For example, sending an email to an employee's personal email address that contains sensitive data is considered negligence and a data breach.
 - 7.4. Intrusion – an external party gains unauthorized access to systems and steals data.
 - 7.5. Leak – a trusted individual or person with access privileges steals or leaks data. For example, someone leaks information to a competitor on our number of phone system sales.
 - 7.6. Loss or Theft – portable USBs, Hard drives, Laptops, Office computers, files and other physical properties are lost or stolen. For Example. Someone drops a USB on the ground and loses it and it contains MCS Civil Pty Ltd (MCS) Sensitive Information.

8. Employee Responsibilities to Prevent a Data Breach

- 8.1. All MCS Civil Pty Ltd (MCS) employees have a responsibility to prevent or report a data breach.
- 8.2. All MCS Civil Pty Ltd (MCS) employees have a responsibility to be diligent with sensitive or PII data. They must take all reasonable steps to ensure information is not subject to a breach. It is the employee's personal responsibility when handling sensitive or PII to ensure this policy standard is upheld.
- 8.3. To assist with this, the below lists some simple Do's & Don'ts to assist employees of the MCS Civil

Pty Ltd (MCS).

8.4. Group to be compliant Do's

- DO report any data breach or potential data breach.
- DO take Data Security seriously.
- DO anticipate data breaches and report if you find a potential concern

Do Nots

- Do NOT leave your computer terminal logged in when walking away. Even to get something from the printer.
- Do NOT forward emails to your personal email address.
- Do NOT leave copies of sensitive or PII on your desk in plain sight if you are in a customer facing area.
- Do NOT give out any of your passwords to anybody
- Do NOT discuss customer specific details with anybody who is not an employee of MCS Civil Pty Ltd (MCS) or a partner of MCS Civil Pty Ltd (MCS) where required
- Do NOT copy files or information onto USB Flash Drives.

9. Reporting of a Data Breach

9.1. Under the Privacy Act 1988 every employee in an organization has a responsibility to report a suspected data breach. This includes all individuals employed by the MCS Civil Pty Ltd (MCS).

9.2. If at any time you believe the above types of information to have been leaked or exposed to a party without authorization you must immediately action the below steps

9.2.1. Raise an IT ticket flagged as urgent and in the stakeholder include

- helpdesk@notjustit.com.au
- nora@mcsaus.com.au

9.2.2. Just like critical IT tickets – if you suspect the data breach is of serious hard or concern, please immediately call the Technical Manager or the Managing Director.

Variations

MCS Civil Pty Ltd (MCS) may regularly review this policy to take account of changes in legislation, activities, services and products. As a result of this review, changes may be made to this policy from time to time and all employees and contractors are required to comply with those changes.

MCS Civil Pty Ltd (MCS) reserves the right to vary, replace or terminate this policy from time.