Systems Data Loss Prevention

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 (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, for example, when conducting an event (collectively referred to as 'workplace').

4. Secure Configuration

4.1. This policy defines what constitutes IT systems secure configuration to protect MCS Civil Pty Ltd and Customer Data. It includes all layers of the OSI model from application configuration to physical configuration. The objective is to prevent data loss across the organisation.

4.2. Please be advised when reading this policy, the scope of the configuration requirements relate specifically to data loss prevention. It is not to be used as a run up guide in any way. The requirements in this policy must be implemented.

4.3. All Windows 10 machines must be enrolled in MCS Civil Pty Ltd Microsoft 365 Intune MDM's group policies.

4.4. Microsoft 365 Intune MDM group policies are reviewed monthly by MCS Civil Pty Ltd Management to ensure compliance with other security policies mentioned.

5. Networking Equipment Configuration

5.1. A Firewall must be implemented at each internet access entry present in the MCS Civil Pty Ltd network. One firewall may service multiple internet connections if its capable of doing so.

5.2. Switches located in staffed areas (eg a small distribution cabinet) must have 'not in use switch ports' disabled to prevent extra devices being plugged in.

5.3. Must have minimum 12-character string gen password. Default password must be changed as soon as the device is turned on and connected to.

5.4. Firewalls to be configured to have real time monitoring which is displayed on a central screen visible by internal IT Staff.

E info@notjustit.com.au **W** www.notjustit.com.au

6. Server, Desktop and Laptop Configuration

6.1. Server, desktop and laptop hardware must be connected to the internal network as soon as they're unboxed.

6.2. Once the device has been initiated on the network, a Monitoring agent under the MCS Civil Pty Ltd security group must be installed straight away.

6.3. The Monitoring agent will remove any 'bloatware' and install only approved applications.

6.4. The default local admin username must be changed once the machine has been configured.

6.5. The default local admin password must be changed to have a minimum 12-character string gen password.

7. Microsoft 365 Configuration

7.1. Desktop, laptop and tablet hardware with Windows 10 installed must be enrolled into MCS Civil Pty Ltd Microsoft 365 Intune MDM tenant as soon as machine is connected to the global internet.

7.2. Microsoft 365 Azure AD groups control the machines access to software as well as data.

7.3. DLP Policy enabled to notify of breaches to the privacy act. Notifications for Drivers Licenses and Passport Numbers being shared to people outside the organisation.

7.4. DLP Policy enabled to notify if any Australian Financial Data shared externally.

7.5. DLP Policy enabled to notify if any PII data shared externally such as TFN or Drivers License number.

8. Anti-Virus Configuration

8.1. Microsoft Defender must be configured so that in a potential data breach situation or a high-risk scenario that it can lock down the USB Ports on the workstations to prevent unauthorised data leaks.

8.2. Microsoft Defender DLP enabled on system and all agents installed on devices.

8.3. Microsoft Defender must be checked regularly to ensure all devices on the network are protected with an antivirus agent.

8.4. For other Anti-Virus configuration requirements please see Anti Malware/Anti-Virus policy.

9. Internal Security Assessments

9.1. Penetration and security assessments must be conducted on a 6-monthly basis on all MCS Civil Pty Ltd locally exposed infrastructure. The following assessments must be completed, and results reviewed by the Chief Risk Officer.

9.1.1. External penetration test

9.1.2. Internal penetration test

9.1.3. Remote access penetration test

9.1.4. Mobile application penetration test

9.2. Any failed tests must be reported to the General Manager as soon as detected and a resolution actioned within 1 hour of detection.

10. External Security Assessments

10.1. Penetration and security assessments must be carried out by all 3rd party cloud applications that MCS Civil Pty Ltd expose any information on. The 3rd party companies are responsible for maintaining and securing their systems, but MCS Civil Pty Ltd is responsible for ensuring compliance with MCS Civil Pty Ltd security standards.

10.2. All 3rd party applications security assessments bust be reviewed by MCS Civil Pty Ltd Chief Risk Officer as soon as their available and/or at a minimum of annually.

E info@notjustit.com.au **W** www.notjustit.com.au

11. Logging Configuration

11.1. Firewalls/Routers/Switches must be configured to log information for a period of 6 months. These must be kept secure and able to be reviewed in case of a data breach situation.

11.2. Server logs must be kept for a minimum of 6 months.

11.3. All other systems which store customer data must have retrievable logs for the previous 30 days.

11.4. All logs must present logical and readable data. The objective with logging is to ensure in a disaster scenario they can be retrieved and understood with relative ease.

12. Data Destruction

12.1. When decommissioning systems, a secure data destruction needs to be completed. This involves ensuring each hard drive in each system has a 3 pass wipe. This 3 pass wipe is completed by MCS Civil Pty Ltd staff using BitRaser for File data erasing software. BitRaser for File is DoD and NATO compliant.

13. Employee Background Checks

13.1. Due to the sensitive nature of the data we handle each day, all employees which start employment with the MCS Civil Pty Ltd must undertake a background check completed by the Chief Risk Officer.

13.2. Any Technical employees which access customers systems and manage customers data must also undertake a criminal record check. If they have outstanding criminal history that relates to impersonation or any other sort of privacy breach, they are unable to be employed in such a role due to the risk.

13.3. It is the responsibility of the HR Manager to ensure these checks are completed. Any red flags must be reported to the Technical Operations Manager.

14. User Training

14.1. Upon Commencement of employment each staff member must complete the Data Classification and Data Loss Prevention training session.

Variations

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

E info@notjustit.com.au **W** www.notjustit.com.au