MUJI Motor Group (Pty)Ltd trading as MUJI Ladysmith

PERSONAL INFORMATION STANDARDS

PoPIA regulates and controls the processing or Personal Information.

MUJI Motor Group strives for the fair and lawful treatment of personal information and this document is intended to support the **MUJI** Data Protection Policy.

Effective Date: 01 July 2021

1. PURPOSE

This policy sets the standard for how **MUJI** Motor Group deals with Personal Information and the commitment to safeguarding of all Personal Information processed by **MUJI** Motor Group and its partners/ service providers.

2. SCOPE

This policy applies to all personal data processed in the course of business by **MUJI** Motor Group.

3. INFORMATION SECURITY

3.1 Applications

Minimum security requirements set out in this standard must be consulted when considering:

3.1.1 Commercial off the shelf applications

3.1.2 Application Development

3.1.3 Security of development and test data

Regular evaluation assessments must be conducted to assess application vulnerability to known security exploits.

This is especially necessary with regard to internet facing applications and sharing portals.

3.2 Infrastructure and network security management

3.2.1 Documentation and configuration management

3.2.1.1 Operating procedures and configuration standards must be recorded and maintained for critical infrastructure and network equipment.

3.2.1.2 Configuration files for critical infrastructure components must be protected from unauthorised access.

3.2.1.3 Hard copy and electronic system documentation must be protected from unauthorised access.

3.2.2 Patch and vulnerability management

3.2.2.1 A formal software update management process must be maintained to ensure up-to-date approved patches have been applied and that hardware and software revisions are still vendor supported.

3.2.2.2 Vulnerability assessments must be carried out on a regular basis and any exposures identified that cannot be addressed with vendor supplied patches must be managed by the application of suitable compensating controls.

3.2.3 Protection against malicious code

3.2.3.1 Critical infrastructure and network equipment must be protected against the effect of malware or malicious code.

3.2.4 Managing wireless networks

*3.2.4.1 Appropriate safeguards must be deployed to prevent the deployment of unauthorised wireless networks at **MUJI** Motor Group.*

3.2.4.2 Authorised wireless networks must utilise strong link layer encryption to prevent unauthorised connections to the network.

3.2.5 Perimeter defences

*3.2.5.1 **MUJI** Motor Group must maintain appropriate perimeter defences. Consideration should be given to both preventative as well as detective mechanisms for perimeter security.*

3.3 Physical Security Management

3.3.1 Secure Areas

3.3.1.1 Critical information processing facilities must be protected by a physical security perimeter, which must be access controlled to ensure no unauthorised access.

3.3.2 Equipment Security

3.3.2.1 Network and infrastructure equipment must be protected from environmental and physical threats.

3.3.2.2 All data and licenced software must be securely erased from equipment prior to disposal or re-deployment.

3.3.2.3 No equipment may be removed without prior authorisation.

3.3.3 Disaster recovery sites

3.3.3.1 Disaster recovery sites must be afforded the same level of protection and production environments.

3.4 Third-Party Security Management (Including Cloud Services)

3.4.1 Security requirements in Service Level Agreements

3.4.1.1 Services delivered by third parties are subject to certain minimum-security requirements which must be detailed in the relevant service level agreements as per section 19 of PoPIA.

*3.4.1.2 If the third party is found to not comply with the security requirements stipulated, **MUJI** Motor Group has the right to terminate the interface between the third-party network and its own.*

3.4.2 Procurement of cloud services

3.4.2.1 The procurement of cloud-based services must be carried out in consultation with IT Department and must meet minimum security provisions stipulated in this policy.

3.4.3 Monitor and review of compliance

*3.4.3.1 To ensure third-party services follow **MUJI** Motor Group security requirements, regular compliance checks and independent assessments are required which will vary per offering, division and purpose*

*3.4.3.2 **MUJI** Motor Group has the right to perform unplanned audits without warning on the third-party information security controls implemented within their environment.*

3.5 Security of Archives and Backup Media

3.5.1 Archives and backup media must be afforded the same level of protection from unauthorised access, loss or disclosure as production data.

3.5.2 The location of backup media and archives must be recorded and tracked.

3.6 Incident Management

3.6.1 Incidents must be managed according to the guidelines of PoPIA.

3.7 Cryptographic Controls

3.7.1 Application of industry grade algorithms where such exist

3.7.1.1 If cryptographic safeguards are required to protect sensitive data and services, only industry recognised protocols with appropriate key strengths and key management may be used.

3.7.2 Key management

3.7.2.1 Cryptographic keys must be managed throughout their lifecycle; generation, sharing, backup, usage, renewal and destruction or archival. Dual control over access to key components is mandatory.

3.7.2.2 Keys must be stored securely.

3.7.2.3 Keys must only be used for authorised purposes by authorised entities or services.

3.7.2.4 Records of all state changes and usage or additional usage of key material must be created and maintained.

4. ACCOUNTABILITY

4.1.1 Information Officer

The **MUJI** Motor Group Information Officer has a primary responsibility to ensure compliance with PoPIA within the MUJI Motor Group and in all the dealings with **MUJI** Motor Group and third-party service providers.

MUJI Motor Group Information Officer is responsible for ensuring compliance in the dealership and that the employees and service providers acting for or on behalf of the dealership understand the role of the Information Protection conditions in their work. This is achieved through induction, training and performance monitoring.

4.1.2 Service Providers

All service providers acting for or on behalf of **MUJI** Motor Group have a responsibility to act strictly in compliance with a duly completed mandate and ensure that processing of Personal Information is carried out in compliance with this mandate and the PoPIA.

5. RETURN OR DESTRUCTION/DE-IDENTIFICATION OF PERSONAL INFORMATION

MUJI Motor Group may at any time, for any reason, request a third party to return all copies of Personal Information in their possession and certify in writing that the personal information has been returned or disposed of securely or de-identified. This applies to written or electronic copies, as well as any other form of media, of personal information.

6. OVERSIGHT/ RIGHT TO AUDIT

MUJI Motor Group must, in all undertakings with third-parties (where feasible), include the right to obtain a network-level vulnerability assessment (or a site audit) based on the recognised industry best practices for information technology and security controls. This must be for all facilities used to process personal information on behalf of **MUJI** Motor Group.

7. MANAGEMENT PROCESS

7.1.1 Any exceptions to this standard must be escalated to the Information Officer.

7.1.2 All contracts must contain provisions relating to Data and Personal Information safeguards.

7.1.3 When **MUJI** Motor Group requires it, all parties should sign a Data Processing and Security Agreement.

8. APPROVAL

This Personal Information Standard is approved by the **MUJI** Motor Group Franchise Director.