Heidelberg Electrical (Pty) Ltd

Organizational Measures Policy for Data Privacy and Protection

---

Heidelberg Electrical (Pty) Ltd advocates and subscribes to best practice of Data Privacy Principles and the protection of Personal Data to ensure the Rights and Freedoms of all people, and various business entitys

---

Organizational Measures Policy for Data Privacy

Contents

Contents 2
1. Purpose 3
2. Application 3
3. Controls 3
3.1 General Compliance 3
3.2 User Access Management 3
3.3 Passwords and PINS 4
3.4 Personal Data Handling 5
3.5 Email and Websites 6
3.6 Incident Management 6
3.7 Agreements 7
3.8 Computers and Devices 8
3.9 Training 8
4. Control Exceptions 9
5. Approval 9
6. Appendix 1 9
6.1 Approved Software 9

Organizational Measures Policy for Data Privacy

1. Purpose

The Organizational Measures Policy for Data Privacy sets out the Information Security and Data Privacy direction and is the backbone of our data privacy and information security posture. The aim of this policy is to proactively and actively identify, mitigate, monitor and manage data privacy and information security threats and risks.

The purpose of this policy is to ensure that our information can be used when required with the confidence that it is accurate, complete and adequately protected from misuse, unauthorized disclosure, damage or loss.

2. Application

This policy and the obligations imposed by it apply not only to employees of our business (whether permanent, fixed or temporary, including directors, principles, executives and leaders), but also any third-parties or sub-contractors providing services to us. In this policy the term “employee” includes all these groups and people.

This policy is applicable to our information assets used to provide and support our business operations.

‘We’, ‘us’ and ‘our’ shall mean all the related bodies corporate or otherwise of the entity known as Heidelberg Electrical (Pty) Ltd

3. Controls

3.1 General Compliance

3.1.1 We do everything that is necessary to ensure that Data that we capture, use, store and manage is always kept secure.

3.1.2 We will always remain alert to physical and technological threats.

3.1.3 We always keep all our computer systems and devices updated with the most recent system updates and patches.

3.1.4 We recognize that Data Privacy may be in paper based information or electronic information.

3.2 User Access Management

3.2.1 We use passwords on all our devices that can apply a password. The passwords that we apply are done so in accordance with control section 3.3 “Passwords and PINS”.

3.2.2 Where possible to access computers, devices, websites and services we will investigate and if appropriate use multi-factor authentication to access these devices and services.

3.2.3 We will configure all our computing devices, such as desktop and laptop computers to automatically lock after 10 minutes of inactivity.

3.2.4 We will configure all our mobile telephony devices, such as tablets and mobile phones to automatically lock after no more than 2 minutes of inactivity.

3.2.5 We will, where possible, configure our devices to lock for a period of 30 minutes if the password or PIN to access the device is entered incorrectly 5 times.

3.3 Passwords and PINS

3.3.1 We will never give our passwords or PINS to anyone. They are confidential and will never be shared.

3.3.2 We must use password generation rules that ensure that our passwords are hard to guess and easy to remember.

3.3.3 Our passwords must be at least 8 Characters long, where possible.

3.3.4 As part of our security measures, we will change our passwords every 90-days, or at least 4 times each year.

3.3.5 We use a unique password and user name combination for each new service, website or subscription that we engage in.

3.3.6 Our passwords must contain at least the following;

(a) 1 x Uppercase A – Z character

(b) 1 X Lowercase A – Z character

(c) 1 X 0 – 9 Digit

(d) 1 X Special Character which may include (“!@#$%^&*()_-+=”)

3.3.7 We will use strong-passwords based on 3.3.6 wherever possible.

3.3.8 When the service, application or password facility presented can accept a “Pass-Phrase” we will use this facility.

3.3.9 We will never write our passwords down, furthermore, if provided for we will use a software Password Vault or Locker application described in Item 6.1.1.

3.3.10 All our devices fixed, mobile and network relation in our business will use a Password or PIN.

3.3.11 If our devices are equipped with Biometric scanners for either Eye (Retina), Thumb (Finger), Palm or Facial Recognition, we shall use that facility.

3.4 Data Handling

3.4.1 When we are a Controller we will;

(a) Not share our data with anyone that the Data Subject is not aware of; If we need to share the Data Subjects Data, we will advise them of this requirement and seek approval prior to allowing the sharing to occur;

(b) Always provide clear concise Collection Statements to our Data Subjects;

(c) Deal with our Data Subjects with a professional level of courtesy; and

(d) Ensure that all the Processors that we use are Data Privacy compliant, and that they have agreed to ensure the Rights and Freedoms of Data Subjects in a manner and way like the way that our business does;

3.4.2 When we are a Processor we will;

(a) Never share Data that is entrusted to us by a Controller;

(b) Ensure that the Data is only used according to the instructions provided by the Controller;

(c) Return or destroy the Data at the written request of the Controller;

(d) Only perform the instructions from the Controller, once they are in writing; If we don't clearly understand such instructions, we shall seek clarity from the Controller, before processing the instructions.

3.4.3 We will not make unnecessary copies of Data;

3.4.4 We will backup the Data in our business no less than 3 times week to a readily available encrypted Disk Drive / Drives / Storage.

3.4.5 When we back up as described in 3.4.4, we shall ensure that the backup is password protected using the processes and password rules described in Control Section 3.3 “Passwords and PINS”.

3.4.6 We will verify our data backups at least once every month to ensure their integrity and the integrity of the disaster recovery process.

3.5 Email and Websites

3.5.1 We will never open an attachment on an email that we weren’t expecting.

3.5.2 We will never click on any links, images or anything else that is contained in an email that we weren’t expecting.

3.5.3 We will not work with Data on websites that don’t have a valid SSL certificates.

3.5.4 We will separate our work and private email by using more than one email account.

3.5.5 Our work-related emails will be stored on encrypted storage devices.

3.6 Incident Management

3.6.1 When we are working with a Controller, we will immediately advise the Controller in the event of;

(a) A data breach in which the Controller’s Data Subjects have been affected;

(b) A request from a Controller’s Data Subject for any changes or deletion, but we will not act on this request, until instructed by the Controller as described in 3.4.2(d);

3.6.2 We will evaluate the most appropriate action and course to take if a computer or device in our business gets a virus that we can’t remove. Such action may include deleting / formatting the infected computer and / or restoring it from an uninfected backup.

3.6.3 If we can’t restore the computer without loss of Data in item 3.6.2, when the lost Data is provided as subject to a Controller and Processor Agreement,

where we are the Processor, we shall immediately notify the Controller under item 3.6.1(a).

3.6.4 If our computing environment is compromised and there is any increased risk to Data, we shall take all steps to minimize the potential impact to all Data Subjects.

3.6.5 If we are using a computer or device that is compromised, and that device contains Data, where we are the Processor, we shall notify the Controller immediately under item 3.6.1(a).

3.7 Agreements

3.7.1 When we are acting as a Controller, we will only work with Data Privacy compliant Processors and ensure that an agreement that accurately describes the processing and services that we are seeking from the Processor.

3.7.2 When we are acting as a Processor, we will only work Data Privacy Compliant Controllers and ensure that an agreement that accurately describes the contacts and compliance status of the Controller.

3.7.3 When we are a Processor, we will never assume responsibility for the Data Subject Request management or process.

3.7.4 We will only select to work with third-party providers that comply with recognized Data Privacy compliance principles and are appropriately certified. Such services will include;

(a) Cloud Service Providers;

(b) Authorized Repairers;

(c) Contractors and Consultants, that will see our Data;

(d) Office Services Companies;

(e) Security Companies;

(f) Processors;

(g) Controllers;

(h) Recipients;

(i) Removal Companies; and

(j) Other business-related services providers that we may engage.

3.8 Computers and Devices

3.8.1 We keep our computers and devices updated with the latest security patches and updates, as directed and issued by the manufacturer. This will include;

(a) BIOS and Firmware updates;

(b) Operating Systems;

(c) Software and Applications; and

(d) Systems and Services;

3.8.2 We will allow our update process to complete at least once each week, if it is scheduled the computers and devices will be left turned on.

3.8.3 We will only install software from credible sources, and our security and threat software and services are as follows;

(a) We will only use Anti-Virus Software as described in item 6.1.2;

(b) We will only use Disk Encryption Software as described in item 6.1.3;

(c) We will only use Threat Management Software as described in item 6.1.4;

(d) We will only use Firewall Software as described in item 6.1.5; and

(e) We will only use Data Backup Software as described in item 6.1.6.

3.8.4 All our disk drives, including any portable and USB drives will be encrypted with the software described in 3.8.3(b).

3.8.5 All our devices, where possible will use Anti-Virus software described in 3.8.3(a).

3.8.6 All our devices, where possible will use Threat Management software described in 3.8.3(c).

3.8.7 All our devices, where possible will use Firewall software described in 3.8.3(d).

3.8.8 We will destroy the content on a device before we dispose of it, ensuring that is it “factory reset” before disposing of it.

3.9 Training

3.9.1 Our employees will be trained to a Data Privacy compliant level when they are handling any Personal Data.

3.9.2 We will train new employees in Data Privacy Handling and Data Privacy principles as part of our onboarding process.

3.9.3 We will retrain our employees in Data Privacy and Protection at least once every 12 months.

4. Control Exceptions

All exception requests must be reviewed and assessed against this policy to identify and ensure that the impact of the exception does not fundamentally alter or change the purpose or intent of this policy document. All Control Exceptions will be recorded in the Exception Register. The exception Register must be submitted as an active part of this policy.

5. Approval

Document Approved By: Jacques McClintock

Document Approval Date: 21-July-2021

6. Appendix 1

6.1 Approved Software

6.1.1 We have approved the use of Microsoft Vault as a Password Vault or Locker Tool in our business.

6.1.2 We have approved the use of Eset Antivirus as our Anti-Virus software in our business.

6.1.3 We have approved the use of Eset Disk Encryption as our Disk Encryption software in our business.

6.1.4 We have approved the use of Eset Antivirus / Internet Security as our Threat Management software in our business.

6.1.5 We have approved the use of Eset Internet Security as our Firewall software in our business.

6.1.6 We have approved the use of Proxmox Backup Server as our Data Backup software in our business.