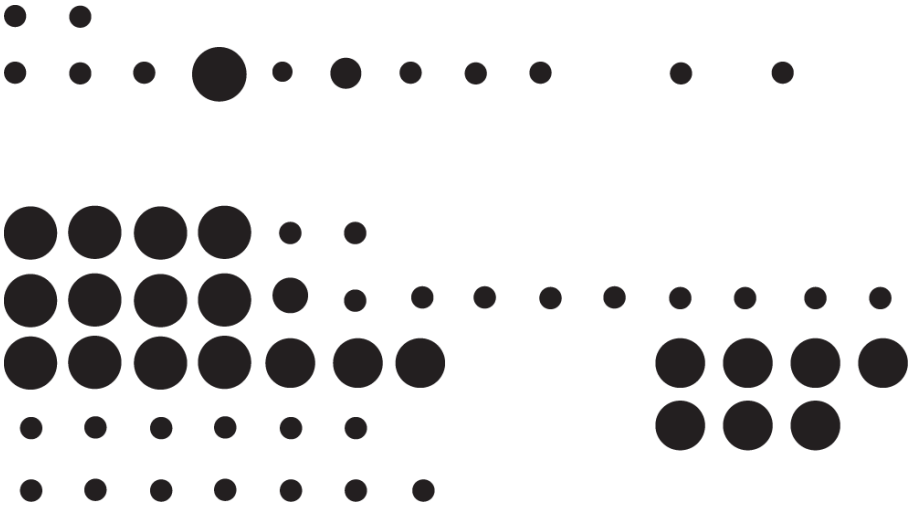
dimension data



Acceptable Use Policy

Name: Acceptable Use Policy

Owner: Chief Information Security Officer

Status: APPROVED

Version: 1.00

Date: 15 February 2021

Review: 15 February 2022

Dimension Data South Africa. The Campus, 57 Sloane Street,
Bryanston, Johannesburg. Tel: +27 11 575 000

Dimension Data contact details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

Dimension Data (Pty) Ltd
The Campus,
57 Sloane Street,
Cnr Sloane Street & Main Road,
Bryanston,
Johannesburg

☏ 011 575 0000
✉ dimensiondata@dimensiondata.com

Terms and conditions

As defined by Dimension Data Information Security classification requirements this document is classified for General distribution. This classification permits sharing with employees, business guests and external partners, it does not mean it is available for public consumption.

© Dimension Data 2020

Table of Contents

© Dimension Data 2020

1. Information Security Foreword

1.1. Introduction

Dimension Data (Pty) Ltd ('Dimension Data') is committed to the implementation of processes and systems to protect and safeguard the Confidentiality, Integrity and Availability ('CIA') of all critical information (including Personal Data) and information processing assets. Providing protection from internal and external threats is in the interest of all our stakeholders and ensures secure service delivery.

1.2. Purpose

The Acceptable Use Policy establishes and communicates the proper and effective use and protection of the company's assets, including computer and telecommunication resources, services, IT infrastructure and what the assets can be used for. All users of such resources, services or assets have the responsibility to use them in an efficient, effective, ethical, and lawful manner.

1.3. Objective

The objective of the Acceptable Use Policy is to provide all Dimension Data users, regardless of their location, with a clear understanding of what are considered acceptable and unacceptable behaviour and practices in the use or interaction with:

- Dimension Data and client information.
- Applications, systems, databases, computing devices, and network resources owned by or operated by Dimension Data.

The policy also covers IT resources, whether owned by Dimension Data, or belonging to our clients, partners or vendors, which are used in hosting and managed services, including:

- Infrastructure as a Service (IaaS).
- Platform as a Service (PaaS).
- Software as a Service.
- Service as a Service

© Dimension Data 2020

2. Acceptable Use Policy

Information is an asset that is critical to the successful operation of the Dimension Data global business and attainment of its business goals. Like all major organisations, Dimension Data makes extensive use of Information Technology (IT) to process this information and it is therefore essential that IT continues to deliver the business benefits that its purchase intended. Any devices used to store, process or transfer Dimension Data data will be subject to monitoring as per Workplace Surveillance Policy.

2.1. Unlawful or Unethical Use

Policy: The organisation's assets, resources, services and property shall not be used in an unlawful, unethical or inappropriate manner. Failure to comply may result in disciplinary action, in line with regional employment regulations and may extend up to and including termination of employment.

2.2. Personal Use

Policy: All corporate assets, including IT infrastructure, services and facilities are provided for the organisation's business operation. Reasonable personal use may be permitted, conducted in employees' own time, and must comply with all the restrictions set out in this and other standards and policies.

2.3. Reporting Information Security Incidents

Policy: If any employee becomes aware of a security incident using the organisation's assets, they must report the incident through the organisation's Security Incident Management system.

2.4. Systems and Media

Policy: All systems and media used to store, process or transfer Dimension Data data must be authorised by Dimension Data including portable and cloud storage.

Policy: No personal cloud storage must be used for Dimension Data data.

Policy: All Dimension Data data and systems provided by the organisation must be returned when no longer required for approved business use.

Policy: Unwanted or unrecognised removable media (CD, DVD, USB sticks, external hard disks etc.) must be securely disposed of in line with the Dimension Data classification and handling policies.

© Dimension Data 2020

2.5. Deployed Systems

Policy: Staff are not permitted to bypass established security safeguards, controls, procedures, or measures or to modify hardware or software solutions

2.6. Access Rights and Privileges

Policy: All staff must adhere to the organisation's authorisation process to obtain the correct access rights and privileges. The ability to access systems, including access through a network, does not imply a right to connect to those systems or to make use of those systems unless authorised.

2.7. Handling Information and Data

Policy: Dimension Data employees must comply with the information classification and handling policy which addresses all issues regarding printing, exchange, disclosure, disposal or scanning of data or information whatever its form and format.

2.8. Software Licensing

Policy: Dimension Data must comply with all software licenses. Acquisition of software or software packages for internal deployment and usage are subject to change management and must only be purchased and deployed through approved IT and procurement channels.

2.9. Mobile Working

Policy: Dimension Data users shall take specific consideration for risk and information security in the utilisation of the organisation's information, infrastructure and services outside of its premises and must comply with the organisation's teleworking policy.

2.10. Clear Desk / Clear Screen

Policy: All staff must secure any sensitive material and removable media when away from their workstation and at the end of each business day and must lock the computer or engage a password protected screen saver when away from their workstation.

© Dimension Data 2020