Document Title: Network Security Basics

Network security involves policies, processes, and practices designed to protect networks,

data, and systems from unauthorized access, misuse, or attacks.

Key Concepts:

- Firewalls filter incoming and outgoing traffic based on rules.

- Intrusion Detection Systems (IDS) detect signs of malicious activity.

- Encryption ensures that data remains confidential during transmission.

- Access control restricts user permissions and system interactions.

Real-World Example:

A company uses a firewall to block malicious IP ranges, employs IDS tools to monitor traffic

patterns, and encrypts sensitive data exchanged with clients.

Purpose:

This document is created solely for testing the Document Understanding RAG System.