

Information Security within dfcu Bank – Policy Statement

Purpose

At dfcu bank, we understand that information security is fundamental to our success and essential for protecting our customers, employees, and stakeholders. We are committed to safeguarding information assets, maintaining customer trust, and enabling secure, resilient business operations in an evolving digital landscape.

Top Management Commitment

Our leadership is fully dedicated to embedding security into every aspect of the bank's operations. We foster a culture of shared responsibility, where all employees, suppliers, and third parties play an active role in protecting sensitive information. We pledge to provide the necessary resources, training, and oversight to maintain the effectiveness of our Information Security Programme.

Information Security Objectives

1. **Establish a Robust Information Security Programme:** Implement and maintain a structured approach to managing security risks and ensuring compliance with industry standards.
2. **Achieve and Maintain ISO 27001 & PCI DSS Certifications:** Attain and maintain globally recognized security certifications to build customer confidence and meet regulatory requirements.
3. **Strengthen Technical Security Controls:** Continuously enhance our defenses to safeguard against evolving cyber threats and minimize the risk of data breaches.
4. **Risk and Compliance Management:** Proactively assess and treat security risks, ensuring compliance with applicable laws, regulations, and contractual obligations.
5. **Improve Security Awareness:** Deliver ongoing training and awareness programs to empower employees and other interested parties to recognize threats and act as the first line of defense.
6. **Social and Economic Impact:** Contribute to financial stability cybersecurity consciousness, and customer protection, reinforcing the bank's reputation as a responsible and secure financial institution.

Commitment to Compliance and Improvement

dfcu Bank is dedicated to complying with all relevant legal, regulatory, and contractual requirements related to information security. We continuously review and improve our security practices to adapt to emerging threats, evolving business needs, and the feedback of our stakeholders.

By adhering to these principles, we demonstrate our unwavering dedication to protecting the bank's information assets and preserving stakeholder trust.

Yours sincerely,



[Charles Mudiwa \(09/04/25 11:10 GMT+2\)](#)

Charles Mudiwa

Chief Executive Officer







ISMS-DOC-05-3 Executive Support Letter

Final Audit Report

2025-04-09

Created:	2025-04-08 (East Africa Time)
By:	Deo Otieno (dotieno@dfcugroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA6vRdS736ROWoHuaSPpUfGyVGw8vYuehA
Documents:	ISMS-DOC-05-3 Executive Support Letter.docx (1 page)
Number of Documents:	1
Document page count:	1
Number of supporting files:	0
Supporting files page count:	0

"ISMS-DOC-05-3 Executive Support Letter" History

-  Document created by Deo Otieno (dotieno@dfcugroup.com)
Documents: ISMS-DOC-05-3 Executive Support Letter.docx
2025-04-08 - 12:39:01 GMT+3- IP address: 102.207.221.119
-  Document emailed to Charles Mudiwa (cmudiwa@dfcugroup.com) for signature
2025-04-08 - 12:41:34 GMT+3
-  Email viewed by Charles Mudiwa (cmudiwa@dfcugroup.com)
2025-04-09 - 12:09:50 GMT+3- IP address: 41.81.80.75
-  Agreement viewed by Charles Mudiwa (cmudiwa@dfcugroup.com)
Documents: ISMS-DOC-05-3 Executive Support Letter.docx
2025-04-09 - 12:09:57 GMT+3- IP address: 41.81.80.75
-  Document e-signed by Charles Mudiwa (cmudiwa@dfcugroup.com)
Documents: ISMS-DOC-05-3 Executive Support Letter.docx
Signature Date: 2025-04-09 - 12:10:19 GMT+3 - Time Source: server- IP address: 41.81.80.75
-  Agreement completed.
2025-04-09 - 12:10:19 GMT+3

