KEYSTONE BANK COOKIE POLICY

This Cookie Policy explains how we use cookies and similar tracking technologies on our website. By accessing or using our website, you consent to the use of cookies and other tracking technologies as described in this Policy.

How We Use Cookies

We use cookies for the following purposes:

a) Essential Cookies: These cookies are necessary for the operation of our website. They enable basic functions such as page navigation and access to secure areas of the Website. Without these cookies, the Website may not function properly.
b) Analytics Cookies: We use analytics cookies to collect information about how visitors use our website. This helps us analyze data and improve the performance and functionality of the Website. The information collected by these cookies is aggregated and anonymous.
c) Advertising Cookies: Advertising cookies are used to deliver personalized advertisements based on your interests and browsing behavior. They may also be used to measure the effectiveness of advertising campaigns.
d) Social Media Cookies: These cookies allow you to share content from our website on social media platforms or enable you to log in using your social media credentials.

Third-Party Cookies

We may also use third-party cookies on our web pages. Third party cookies are cookies provided by third-party service providers. These cookies are subject to the respective privacy policies of these providers. We have no control over these cookies, or the data collected through them.

Cookie Settings

You can control and manage cookies preferences through your browser settings. Most browsers allow you to block or delete cookies. However, please note that blocking or deleting cookies may affect your ability to access and use certain features of our website.

IT Services Management Systems Policy:

The IT Service Management Systems Policy for Keystone Bank aims to establish guidelines and procedures for the effective management and delivery of IT services. Its main purpose is to ensure the effective management and delivery of IT services within Keystone Bank, and it applies to all IT services provided by Keystone Bank.

This policy aims to ensure the alignment of IT services with business objectives, effective incident and change management, proactive problem resolution, accurate configuration management, resilience in the face of disruptions, and robust security measures to protect sensitive data and infrastructure.

Our IT services align with strategic business objectives, with established SLAs for our critical services in line with best practices outlined in the ISO IEC 20000:2018 standard.

We have developed standardized process for identifying, prioritizing, and resolving IT incident, our change management processes are formalized to manage and control changes to our systems thereby effectively minimizing business disruptions.

Information System Management Standard Policy

The Information System Management Standard Policy for Keystone Bank aims to ensure the security and integrity of its information assets through compliance with ISO 27001 standard. Its main purpose is to recognize the importance of Information Security Management System (ISMS) in safeguarding information assets and establishes a framework for ISO 27001 compliance and continual improvement. It applies to all individuals associated with Keystone Bank who access, manage, or handle its information assets.

Keystone Bank is committed to establish, implement, maintain, and continually improving an ISMS in accordance with ISO 27001 standards. By Identifying and assessing information security risks and implementing controls to mitigate these risks and protecting the confidentiality, integrity, and availability of information assets through technical, organizational, and procedural security measures.

Our policy aligns with ISO IEC 27001:2022 standard to ensure robust protection of its information assets to monitor, measure, and evaluate the effectiveness of the ISMS through regular audits, reviews, and assessments. To continuously improve the ISMS based on audit results, reviews, assessments, and changes in the business environment and technology landscape.

Business Continuity Policy Standard:

The Business Continuity Policy of Keystone Bank highlights the crucial need to maintain operational resilience amidst emergencies, calamities, and operational interruptions. It establishes a framework for crisis management, disaster recovery planning, and business continuity management to ensure the integrity and continuity of operations.

Our business continuity framework and processes are tailored according to the ISO 22301:2019 standard which is a world class standard for managing an effective business continuity system.

Keystone Bank has implemented a comprehensive governance framework to oversee these processes, emphasizing the bank's commitment to effectively managing and mitigating risks to ensure business continuity.

Data Privacy Policy:

Keystone Bank prioritizes the security and privacy of employee, customer, and third-party data, adhering to data protection laws. The policy encompasses procedures for collecting, using, disclosing, and safeguarding personal data, applicable to all data collected during business operations. Personal data is processed only for legitimate business objectives, gathered transparently either directly from individuals or through legal means. The bank employs technical and organizational measures to prevent unauthorized access, disclosure, or alteration of data, supplemented by regular risk assessments to address potential security vulnerabilities.