



## RAKBANK-Internet Usage Guide Lines

Document Title	RAKBANK-Internet Usage Guide Lines
Creation Date	02 Nov 2006
Last Update	20 Feb 2024
Owner	Information and cybersecurity

### Disclaimer

The content of this Document is intended solely for the use of the individual or entity to whom it is addressed and any others who are specifically authorized to receive it. It may contain confidential or legally privileged information. You are hereby notified that any disclosure, copying, distribution or otherwise placing reliance on the contents of this information is prohibited and may be unlawful in certain legal jurisdictions. The content of the following document are the property of **RAKBANK**. It is provided for the users of **RAKBANK** to use as a reference as to comply with Bank's Information and cybersecurity policies when necessary. **RAKBANK** reserves the right to add and/or delete material from this document at any time.

## Document Control



Version	Date Issued	Status	Prepared by	Change Reason
1.0	02.11.2006	Issue	Infosec	
1.1	12.01.2009	Issue	Infosec	Review and No updates.
2.0	18.01.2010	Issue	Risk and Assurance	Review and No updates
3.0	31.03.2011	Issue	Risk and Assurance	Annual Review and added social networking websites usage
3.1	15.05.2011	Issue	Sr. Manager Information Security and System Planning	Updated Distribution and approval lists
3.2	07.09.2011	Issue	Sr. Manager Information Security and System Planning	Updated Department name from IT Security to Information Security and System Planning
3.3	07.04.2012	Final	Sr. Manager Information Security and System Planning	RACI Matrix Updated
4.0	07.10.2012	Final	Sunil Kumar Sharma	Yearly review
4.1	21.01.2014	Final	ISD	Yearly review
5.1	12.11.2015	Final	ISD	Yearly review
5.2	10.11.2016	Final	ISD	Yearly review
5.3	29.11.2017	Final	ISD	Yearly review
5.4	14.11.2018	Final	ISD	Yearly Review
5.5	13.10.2019	Final	ISD	Updated Distribution and approval lists
5.6	18.02.2020	Final	ITRMFP	Yearly Review
5.7	22.02.2021	Final	ITRMFP	Yearly Review
5.8	16.02.2022	Final	ITRMFP	Annual Review
5.9	13.03.2023	Final	ISC	Annual Review, department name change and removal of LinkedIn from Social Media Sites
6.0	20.02.2024	Final	ICS	Annual review and department abbreviation change

## Distribution List

Name	R/A/C/I
Vice President- Information and Cybersecurity Governance	R
Executive Vice President & Head -Information, Cyber Security and Fraud Prevention	A

Note: R = Responsible, A = Approval, C = Comment, I = Information only

## Document Sign-off

Name	Designation	Signature and Date
Rahul Mishra	Vice President- Information and Cybersecurity Governance	 22/02/2024
Tushar Vartak	Executive Vice President & Head - Information, Cyber Security and Fraud Prevention	 22 FEB 2024

## Table of Contents

<b>Document Control.....</b>	<b>2</b>
<b>Distribution List.....</b>	<b>3</b>
<b>Document Sign-off.....</b>	<b>3</b>
1 Internet Usage Guidelines.....	5
2 Personal Responsibility .....	5
3 Term of Permitted Use .....	5
4 Purposes and Use .....	5
5 Sending and Receiving Files.....	6
6 Banned Activities.....	6
7 Confidential Information .....	7
8 Privacy .....	7
9 Non-compliance .....	7
10 Employee Acknowledgment .....	7



## **1 Internet Usage Guidelines**

RAKBANK enables Internet access to some of its employees to undertake activities specifically related to their jobs. It is not provided for personal convenience. These guidelines apply to those who have been granted Internet access.

Upon acceptance of your agreement to follow these guidelines, you will be granted Internet access. The use of the Internet access facility is for the specific use of the authorized individual and is not to be shared with other members of staff or people external to the organization.

Any breach of these guidelines will result in your Internet access being withdrawn. In addition, it may be referred to Human Resources department for disciplinary action.

## **2 Personal Responsibility**

By signing Internet usage guidelines, you agree to adhere to the Acceptable use policy. You also agree to report any Internet misuse to the Information and Cybersecurity Department

## **3 Term of Permitted Use**

Use of the Bank's corporate network is governed by the Information security policy, so please make sure you are aware of the Information security policy of the Bank, which is available on the "Information and Cybersecurity" section of RAKNet.

## **4 Purposes and Use**

Internet access is provided as a tool to accomplish the Bank's business objectives. If you are unsure whether an activity constitutes appropriate business use, follow the guidelines outlined below or consult either Vice President - Information and Cybersecurity Governance or IT Helpdesk. Internet access is monitored such that it is possible to monitor the web sites visited by each user and when. Additionally, various web sites such as web email and sports sites have been blocked. Further to this, based on the usage and content, other sites may be blocked without notice

## **5 Sending and Receiving Files**

The Bank will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined below.

## **6 Banned Activities**

The following activities violate Bank's Internet usage guidelines: -

- a) Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language and materials.
- b) Making ethnic, sexual-preference, or gender-related slurs or jokes.
- c) Accessing social networking websites like Facebook, Twitter and Instagram etc.
- d) The following are considered to be a violation of Information Security policy such as:
  - Sharing confidential material, trade secrets or proprietary information outside of the organization including customer confidential information.
  - Conducting any sort of personal business.
  - Viewing, transmitting, downloading, or searching for obscene, pornographic, materials.
  - Sending test data or samples to vendors without obtaining appropriate approval.
  - Using software that is not licensed or approved by RAKBANK
  - Downloading viruses, worms, other harmful component, or corrupted data to vandalize the network.
  - Downloading or transmitting copyrighted materials without permission from the copyright holder.
  - Even when materials on the network or the Internet are not marked with the copyright symbol, ©, employees should assume all materials are protected under copyright laws unless explicit permission to use the materials is granted.
  - Using another employee's password to deceive the recipients into believing someone other than you is communicating or accessing the Internet.
  - Representing personal opinion as those of the Bank.
  - Attempt to gain illegal access to remote system on the Internet.
  - Use or possess Internet scanning or security vulnerability assessment tools without permission or approval of the management.
  - Establish Internet or other external network communication that could allow external users to gain access into bank's system and information assets.
- e) Endangering the security and access to the Bank's network or other Internet networks by disclosing or sharing passwords or impersonating others. Users will be prevented from downloading or installing Active-X or Java controls, which are not authorized by IT department. Only the IT department is authorized to install any software, even if it is available free of cost. Freeware or Shareware programs should not be downloaded through Internet access. No programs should be installed without appropriate approvals.
- f) Accessing or attempting to access controversial or offensive materials. Internet access may expose employees to illegal, defamatory, inaccurate, or offensive materials. Employees must avoid these sites.

## **7 Confidential Information**

Users of this facility are prohibited from unauthorized disclosure of Bank's confidential information, its staff or its clients. In the same way, they are prohibited from revealing internal IP address or network related details without any authorization.



## 8 Privacy

Internet access is provided as a tool to accomplish the organization's objectives. Any content legitimately downloaded in accordance with these guidelines becomes the property of RAKBANK. Network administrators may review files and intercept communications for any reason, including, but not limited to, maintaining system integrity and ensuring employees are using the system in accordance with these guidelines.

## 9 Non-compliance

Internet access is a privilege, not a right. Internet access assigned to user may be withdrawn upon any violation of these guidelines and may be subject to disciplinary action in compliance with the Bank's Disciplinary Procedure.

Acceptable use policy breaches include violating the above provisions and failing to report violations by other users. Permitting another person to use your account or password to access the Internet facility will be considered as a violation of these guidelines.

## 10 Employee Acknowledgment

*Note: If you have questions or concerns about these guidelines, contact IT Helpdesk or Information and cybersecurity department before signing this agreement.*

I have read Internet usage guidelines and agree to abide by it. I understand that any violation of the above terms may be subject to disciplinary action.


Employee Name

Vinayak Singhal

Employee Number

IT1549

Employee Signature & Date

 13/9/24