

Document name	End User Information Security
Document number	POL-IS-002 Version 4.0

Contents

1. Purpose	1
2. Policy	1
3. Declaration	4

1. Purpose

It is the responsibility of every user (direct employee, consultants or temporary staff) to safeguard the information assets of Al Hilal Bank ('the bank'). This policy outlines the standards each user must abide by in order to protect the bank's information asset.

The desired objectives of the policy are to ensure that all end users adhere to the Information Security requirements and ensure that banks information remains secure at all times.

2. Policy

2.1 General use of Ownership

- 2.1.1 Users should be aware that all data they create on bank's systems remains the property of the bank.
- 2.1.2 All users of the bank's information systems shall be responsible and liable for all actions including transactions, information retrieval or communication performed on the bank information systems by using their user ID(s) and password(s).

2.2 User Identification

- 2.2.1 Every user shall have a uniquely assigned login name and password to access the bank's computer systems.
- 2.2.2 Each employee is responsible for the login name/password assigned to him/her.
- 2.2.3 For the issue of a new login name, a signed form indicating the relevant privileges is required, either in hardcopy or as part of the internal workflow software like Assyst should be submitted.
- 2.2.4 User login will be locked after three (3) unsuccessful attempts and reactivated either after a minimum of 30 minutes or upon request to the IT Service Desk.

2.3 Password

- 2.3.1 All users must ensure that the password selected complies with the following password composition rules:
 - 2.3.1.1 Password shall be minimum eight (9) characters long.
 - 2.3.1.2 Password shall have at least one lower case letter, one upper case letter, one numerical character or special characters (e.g. @#\$%^&*()_+|~-='{}[]:"';<>?./!).
 - 2.3.1.3 Passwords shall not be the same as the last 10 passwords.
- 2.3.2 Password shall be changed every 45 days.
- 2.3.3 Password shall not be a word in any language, slang, dialect, jargon, etc.
- 2.3.4 Passwords shall not be based on personal information, names of family, friends, relations, colleagues, etc.
- 2.3.5 Users shall not share or reveal their passwords to anyone, or write down their passwords on physical or electronic media.

2.4 User Privileges Management

- 2.4.1 A login ID not used for 90 days will be disabled and later deleted with the permission of the employee's Line Manager, Head of Department or Dept. of Human Resources.
- 2.4.2 Line Manager, Head of Department or Dept. of Human Resources must promptly report all significant changes in user duties or employment status to the computer system security administrators handling the user-IDs of the affected persons.



Document name	End User Information Security
Document number	POL-IS-002 Version 4.0

- 2.4.3 Where staff are involuntarily terminated, they must be immediately relieved of all of their duties, required to return all bank's equipment and information, staff's immediate Line Manager, Head of Department or Dept. of Human Resources are responsible for ensuring all access privileges of the staff are promptly revoked.

2.5 Privacy and Personnel Policy

- 2.5.1 The bank reserves the right to examine all information stored in or transmitted by the users.
2.5.2 HR will ensure that the person has all user accounts disabled prior to the employee's final settlement.

2.6 Desktop/Laptop Security

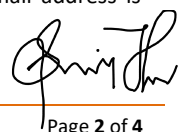
- 2.6.1 Automatic protection features (e.g. password protected screen saver, keyboard lock) in computers shall be activated if there has been no activity for 5 minutes to prevent illegal system access attempt. Alternatively, the logon session and connection shall be terminated.
2.6.2 Confidential and Sensitive Data should be held on File Servers and not on "Local Drives" of the user's PC or on any Removable Media.
2.6.3 No person should leave his/her PC or terminal without logging off or locking their workstation.
2.6.4 All software installed on the PC must be owned by the bank and installations should be carried by IT Service Desk only.
2.6.5 Breach of copyright of a software package may render the user liable to prosecution and/or subject to internal disciplinary actions.
2.6.6 Personal external mass storage devices must not be used without approval from the respective Head of Department and Head of Information Security Compliance. External mass storage device includes, but not limited to, USB drives, flash memory, and compact discs. Encryption must be used on those devices to protect from unauthorized access to this information in case the device is lost or stolen.
2.6.7 Employees in possession of laptop, portable computer or mobile computer devices for business purposes shall safeguard the equipment in his/her possession, and shall not leave the equipment unattended without ensuring prudent security measures.
2.6.8 All users with Laptop shall use locks (Kensington Lock) to physically lock such equipment.
2.6.9 Users must not connect their personal owned computers to corporate LAN.

2.7 Network Security

- 2.7.1 Users are prohibited from connecting dial-up modems (external and internal modems) or Wi-Fi to workstations, which are simultaneously connected to a local area network (LAN) or another internal communication network.
2.7.2 Wireless networks shall not be enabled on desktop computers or any devices connected to bank's corporate network unless approved by Head of IT and Head of Information Security Compliance.

2.8 Email Security

- 2.8.1 Any electronic mail address or account associated with the bank, assigned to the users becomes the property of the bank.
2.8.2 Permission to send emails to outside mail addresses shall be provided to those staffs that have a need to do business using the email outgoing facility. Staff requesting the ability to send emails to non-Al Hilal Bank email addresses should be approved by the Head of Department and Information Security Compliance.
2.8.3 Internet based public E-mail systems such as Hotmail, yahoo, Gmail etc. are blocked and must not be accessed.
2.8.4 Organization electronic mail systems must not be used to:
2.8.4.1 Send/ Forward sensitive business information to non-Al Hilal Bank mail addresses except for business purposes.
2.8.4.2 Send or forward chain letters, jokes that are discriminatory in nature etc.
2.8.4.3 Send or receive email messages that contain profanity, obscenities, or derogatory remarks discussing employees, customers, or competitors.
2.8.4.4 Send or forward emails with contents that discuss about illegal, unethical or improper activities.
2.8.4.5 Send or forward emails with attachments or embedded images that are pornographic in nature.
2.8.5 The use of 'auto-forward' rules to send internal BANK business e-mail to a non-BANK email address is forbidden. "Blanket forwarding" of emails to non-the bank email address is also forbidden.



Document name	End User Information Security
Document number	POL-IS-002 Version 4.0

2.9 Internet Security

- 2.9.1 Bank's Internet Facility is to be used only for business purposes. Occasional personal use is permissible if the use: (a) does not consume more than a trivial amount of resources that could otherwise be used for business purposes, (b) does not interfere with productivity, and (c) does not pre-empt any business activity.
- 2.9.2 The bank reserves the right to scrutinize the Internet access logs of the employees and any improper usage will be brought to the attention of relevant management.
- 2.9.3 The bank reserves the rights to block access to any Internet sites that are deemed inappropriate. The ability to connect to a specific web site does not imply that users are permitted to visit that site.
- 2.9.4 Users should not download software from the Internet, or other systems outside the entity without the permission of IT Department. This prohibition is necessary because such software may contain viruses, worms, Trojan horses, and other software, which may damage the entity information and systems.
- 2.9.5 The bank's computer systems should not be used to install personal web pages or web servers, server software or database.

2.10 Clear Desks and Clear Screen Policy

- 2.10.1 Staff must ensure that all documents and removable storage media are stored either in designated places, in locked cabinets or other such furniture when not in use especially after business hours.
- 2.10.2 PCs and computer terminals must not be logged on when unattended and must be protected by key locks, screen saver passwords and other such controls when not in use.
- 2.10.3 All system screens in the data center must be locked when not in use. All system documentation must be secured.
- 2.10.4 All staff who handles bank's sensitive, confidential, or private information must adequately conceal this information from unauthorized disclosure to nearby non-authorized parties such as customers or other third parties.

2.11 Software license agreements

- 2.11.1 Software license agreements must be strictly adhered to. Proprietary software cannot be duplicated, modified, or used on more than one personal computer except as expressly provided for in the manufacturer's license agreement.
- 2.11.2 No pirated / unlicensed software should be used on the bank's IT systems.

2.12 Third Party Security

- 2.12.1 The risks associated with third party involvement and outsourcing should be identified and appropriate measures taken to address them.
- 2.12.2 A Non-disclosure agreement is essential before sensitive information is shared with the third party.
- 2.12.3 The role and responsibilities of the third party should be clearly defined.
- 2.12.4 Third party access to the bank's computer system will be given only after the signing of a formal contract, which should contain all security requirements by which the third party is to abide.

2.13 Virus and Malwares

- 2.13.1 It is the responsibility of all users to take the following actions to prevent infection and spread of computer viruses:
 - 2.13.1.1 All virus incidents and cases or suspects of virus detection, must be reported to the IT Service Desk immediately.
 - 2.13.1.2 Portable Media sent, and files (attachments) transferred electronically, from bank's offices must be virus checked before dispatch. (Virus checking must be carried out using the approved virus scanning software installed on each PC.)

2.14 Reporting of Incidents and Problems

- 2.14.1 Users shall report all incidents/problems to IT Service Desk (on +971 2 499 4141) for reporting, follow-up and resolution of Information System related incidents and problems.
- 2.14.2 Users shall report all security related incidents to infosec.alerts@ALHILALBANK.AE.

2.15 Handling Sensitive Information

- 2.15.1 Users shall ensure that all sensitive information transmitted or received through fax, printed or copied on printers and photocopiers are collected from printers immediately.



Document name	End User Information Security
Document number	POL-IS-002 Version 4.0

- 2.15.2 Users should not send confidential or sensitive information (such as cardholder information) unencrypted. While sending card holder information via email to internal or external email addresses and if no encryption is present / used, the middle six digits of the card number (only the first 6 digit and last 4 digit be visible) should be masked as shown in example. Example: Card No: 1234 56XX XXXX 4321

2.16 Physical Security

- 2.16.1 All staff must wear an identification badge on their outer garments, whenever they are in the bank building or related branches, so that the information on the badge is clearly visible and shall remove identification badges outside the premises.
- 2.16.2 Staffs who have forgotten their identification badge must obtain a temporary badge from the Reception. Identification badges and physical access cards that have been lost or stolen--or are suspected of being lost or stolen--must be reported to 600 522229 with an instruction to block the card access.

3. Declaration

The undersigned hereby warrants and represents that he/she as staff member of Al Hila! Bank or seconded ("Employee / Vendor") to Al Hilal Bank ("the Bank"), has read and understood and shall abide by this Acceptable Usage Policy,


S/he will undertake to keep himself/herself abreast with changes to this policy and attend its scheduled security awareness sessions while strictly complying with said policies knowing any negligent or intended deviation will result in disciplinary action including immediate termination of contract or employment; and any intentional deviation from said policies will result in additional disciplinary actions including legal action and criminal proceedings as well.

S/he agrees that these undertakings shall be treated as an integral part of his/her employment agreement with the Bank (whether directly employed by the Bank or seconded to it) noting such undertakings shall survive the termination and/or expiration of her/his employment for a period of five years.

For Staff (AHB / ADCB Group)

Name	Staff ID (AHB / ADCB)	Department Name	Sign / Date
Sridhar Subramani			

For Vendors / Consultants:

Consultant Name (s)	Vendor / Project Name	Project Manager Name	Consultant Sign / Date
Sridhar Subramani			 02/Nov/2022


Nov/2022