Privacy Policy

This Privacy Policy explains how we may collect information from you when you visit our web site or when you use our online financial services.

We recognize the importance our customers place on the privacy and security of their personal information. Our goal is to protect your personal information in every way that we interact with you, whether it's on the telephone, in our branches, or on the Internet.

We think it is important for you to be informed of the policies, procedures, and security measures that we have in place to safeguard your personal and confidential information. With that in mind, we have developed this Privacy Policy to help you to understand the steps we take to protect your personal information when you utilize our online financial services.

In addition to the protections discussed within this Internet Privacy Policy, your online financial activities may also be protected by our General Privacy Policy.

Below are several definitions of terms used within this policy:

Customer Information – Customer Information refers to personally identifiable information about a consumer, customer or former customer of this Institution.

Internet Protocol (IP) Address – an IP address is a unique address that devices use in order to identify and communicate with each other on a computer network. An IP address can be thought of as a street address or a phone number for a computer or other network device on the Internet. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. We may use IP addresses to monitor login activity and for identification purposes when necessary for security investigations.

Cookie – a Cookie is a very small text file sent by a web server and stored on your hard drive, your computer's memory, or in your browser so that it can be read back later. Cookies are a basic way for a server to identify the computer you happen to be using at the time. Cookies are used for many things from personalizing start up pages to facilitating online purchases. Cookies help sites recognize return visitors and they perform a very important function in secure Internet banking.

"Session" Cookies are used to monitor session activity within our Internet banking product. These Cookies are encrypted and only our Service Provider can read the information in these Cookies. The session Cookie facilitates the processing of multiple transactions during a session without requiring you to reenter your passcode for each individual transaction. Session Cookies used within our Internet banking or Mobile App product do not pass to your computer or phone's hard drive. Instead, the Cookie is stored in your computer or phone's memory, identifying only your

computer/phone while you are logged on. When you log off, or close your browser/app, the Cookie is destroyed. A new Cookie is used for each session; that way, no one can use the prior Cookie to access your account. For additional security, the Cookie expires after 1 minute of inactivity. It must then be renewed. We do not use this Cookie to collect or obtain personal information about you.

Service Provider – In order to provide a full range of online financial services, we may use various third party providers. These third parties provide services such as: website hosting, Internet banking, Mobile App, bill payment, and account aggregation. Third party providers are referred to within this policy as "Service Providers".

Information Collected on the Internet

If you are just browsing through our website, we do not request any personally identifiable Customer Information, nor do we collect unique identifying information about you unless you voluntarily and knowingly provide us that information, such as when you send us an email or complete an application online. If you provide us this information, it is only used internally and in furtherance of the purpose for which it was provided.

As part of providing online financial products or services, we may obtain information about our customers and website visitors from the following sources:

- Information we receive from you on applications, emails, or other forms;
- Information about your transactions with this Institution and our affiliates;
- Information we receive from a consumer-reporting agency; and
- Information that is generated electronically when you visit our website or use our online financial services.

Service Providers hosting our website and Internet banking service may collect general information on our website visitors for security and statistical purposes. Such information may include:

- The Internet address (referral site) which brought you to our web site;
- The date and time you access our site;
- The name and version of your web browser;
- Your Internet Protocol (IP) address;
- The pages visited in our website; and
- The duration of your online session.

Our Service Providers may use Cookies to collect some the above information. In some cases you must accept cookies in order to view our website.

When you click on advertisements in our website or advertisements on linked 3rd party web sites, you may receive another Cookie; however, you do not have to accept any Cookies from third party advertisements.

As mentioned previously, our Service Provider(s) may also use Cookies within our Internet banking and bill payment products. You must accept these Cookies in order to utilize the service. These Cookies do not store any personally identifiable information; they simply provide another level of security.

Use of Information Collected

We may disclose the information that we collect, as described above, with Service Providers acting on our behalf to provide online financial services such as Internet banking/Mobile App and bill payment.

We may also disclose Customer Information when required or permitted by law. For example, Customer Information may be disclosed in connection with a legal process, fraud prevention, or security investigation.

We may also share Customer Information outside this Institution when we have your consent, such as when you request a specific product like insurance or an investment product from a third party financial services provider.

We may also disclose aggregate (not personally identifiable) Customer Information with Service Providers or financial institutions that perform marketing and research services on our behalf and with whom we have joint marketing agreements. Our contracts require all such Service Providers/or financial institutions to protect the confidentiality of your Customer Information to the same extent that we do.

We do not disclose any Customer Information about our customers, former customers, or website visitors to anyone, except as permitted or required by law.

We do not sell any of your personal information.

Account Aggregation

Account aggregation sites allow you to consolidate account information from several sources into one online location. In order to provide this service, an aggregation provider may request your passcode and login information. You should ensure that the aggregation provider has appropriate policies to protect the privacy and security of any information that you provide.

If you provide information about your Meezan Bank accounts to an aggregation provider, we will consider all transactions initiated by an aggregator using the access or login credentials that you provide, to be authorized whether or not you were aware of a specific transaction.

If you decide to revoke the authority given to an aggregation provider, we strongly recommend that you also change your online passcode with Meezan Bank. This will help ensure that the aggregation company cannot continue to access your account(s) with us.

Email Policies

When you enroll for our online services, we will send you a welcome email. We may also send emails marketing various products and services offered by this Institution..

We will also send security related email notices when you sign-up for email (“notify me”) alerts on your account(s) or whenever you change your passcode, security question, or email address.

If you agree to accept electronic disclosures and/or online account statements, we may also send you notices of important account updates through email. For example, if you have agreed to accept disclosures electronically, we may send you an email with updates to this privacy policy and/or we

may send you a notice that your account statement is available for viewing on our website. For more information on how to enroll for electronic disclosures, please contact us at 111-331-331.

Beware of Phishing Attempts and Internet Scams

While email is convenient and has a good business use, it can also be misused by criminals for scams and various other fraudulent purposes. “Phishing emails” are frequently used by criminals to entice the recipient to visit a fraudulent website where they try to convince the recipient to provide personal information, such as ATM card numbers, account numbers, access IDs and passcodes. Some of these fraudulent websites may also be virus laden and can be used to download mal-ware to your computer. Fraudulent websites often look identical to a legitimate site, so it’s important to look very closely at the website address.

Below we have listed a few tips to help protect your personal information on the Internet:

- Always be wary of links in emails, especially any links in emails purporting to be from Meezan Bank.
- Please remember that if we send you an email, we will never ask for personal information such as your account number, ATM card number, PIN number, or social security number.
- Bookmark financial websites and use these bookmarks every time you visit the website.
- Whenever you enter personal information like your access ID or passcode, always look for the lock symbol, or https: in the address bar. Always click on the lock symbol and review the certificate details.
- Update your Internet browser! Most browsers now offer free anti-phishing tool bars that can help alert you of fraudulent websites.
- If you send us an email, please do not include any confidential, personal or sensitive information in the email message, as email messages are generally not secure. We do offer secure messaging through our Internet Banking/Mobile App product and you may use this secure messaging feature if you need to send us sensitive or confidential information.
- Make sure that your computer always has up-to-date versions of both anti-spyware and anti-virus software.

External 3rd Party Links

Our website may include links to other 3rd party web sites. These links to external 3rd parties are offered as a courtesy and a convenience to our customers. When you visit these sites, you will leave our website and will be redirected to another site.

Meezan Bank does not control linked 3rd party web sites. We are not an agent for these third parties nor do we endorse or guarantee their products. We make no representation or warranty regarding the accuracy of the information contained in linked sites. We suggest that you always verify the information obtained from linked websites before acting upon this information. Also, please be aware that the security and privacy policies on these sites may be different from our policies, so please read third party privacy and security policies closely.

While using our website, you may still see our logo when linking to a 3rd party site. A technique called “Framing” allows us to display our logo and look and feel while allowing you to browse another site at the same time. It’s important to note that while you may still see our logo and frame, any information you provide to a 3rd party is not covered by our privacy or security policies.

If you have questions or concerns about the privacy policies and practices of linked 3rd parties, please review their websites and contact them directly. This privacy policy applies solely to the Customer Information collected by Meezan Bank.

Security

Meezan Bank and our Service Providers have developed strict policies and procedures to safeguard your Customer Information. Our policies require confidential treatment of your personal information. We restrict employee access to your personal information on a "need to know" basis and we take appropriate disciplinary measures to enforce employee privacy and confidentiality responsibilities. We have established training programs to educate our employees about the importance of customer privacy and to help ensure compliance with our policy requirements.

Furthermore, Meezan Bank and our Service Providers maintain strong physical, electronic and procedural controls to protect against unauthorized access to customer information. Our computer systems are protected in the following ways:

Computer anti-virus protection detects and prevents viruses from entering our website, email, and computer network systems.

Firewalls and intrusion prevention systems block unauthorized access by individuals or networks.

We use encryption technology, such as Secure Socket Layer (SSL), to protect the transmission of your confidential information. Whenever you login to our Internet banking/Mobile App product or schedule an online transaction through our system, the communication is encrypted. Encryption scrambles transferred data so it cannot be read by unauthorized parties.

We provide secure email through our Internet Banking/Mobile App product to help ensure that your communications with us are confidential.

We continually monitor technological advances and upgrade our systems to ensure your information remains secure.

Customer Awareness for Internet Banking

Recently, Meezan Bank has seen significant changes in the internet banking/Mobile App threat landscape. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls. Various complicated types of attack tools have been developed and automated into downloadable kits. Fraudsters are responsible for losses of hundreds of millions of rupees resulting from online account takeovers and unauthorized funds transfers. Meezan Bank is providing the below security awareness information for your use and action to help protect you online account and transaction information.

Below are the protections and liabilities for consumer transactions using Meezan's internet banking or Mobile App:

To access our Internet Banking/Mobile app service, you must use the Login ID and/or other means of access we establish or provide for your Internet Banking Customer Account together with a Passcode. It is your responsibility to safeguard the Login ID and Passcode. Anyone to whom you give your Login ID and Passcode or other means of access will have full access to your accounts even if you attempt to limit that person's authority

You, or someone you have authorized by giving them your Login ID and Passcode or other means of access (even if that person exceeds your authority), can instruct us to perform the following transactions:

- Make transfers between your accounts to the extent authorized;
- Obtain information that we make available about your accounts;
- Obtain other services or perform other transactions that we authorize.

You must have enough money or credit in any account from which you instruct us to make a payment or transfer. You also agree to the Terms & Conditions of your deposit account that you received when you opened your deposit account.

STATEMENTS

Your Internet Banking/Mobile App payments and transfers will be indicated on the monthly or quarterly statements we provide. Please notify us promptly if you change your address or if you believe there are any errors or unauthorized transactions on any statement, or statement information.

UNAUTHORIZED TRANSACTIONS OR LOSS OF THEFT OF YOUR INTERNET BANKING/Mobile App ID OR PASSCODE

If you believe your Login ID or Passcode or other means of access have been lost or stolen or that someone has used them without your authorization, call us immediately at 111-331-331. Immediately contacting us by phone is the best way of reducing your possible losses. If you have given someone your Login ID and Passcode or other means of access and want to terminate that person's authority, you must change your Login ID and passcode or other means of access or take additional steps to prevent further access by such person.

You are responsible for all transfers you authorize using the Internet Banking/Mobile App services under this Agreement. If you permit other persons to use your account, you are responsible for any transactions they authorize or conduct on any of your accounts. However, tell us at once if you believe anyone has used accessed your accounts without your authority. Telephoning is the best way of keeping your possible losses down.

Limitation of Liability for Internet Banking/Mobile App Services. If we do not complete a transfer to or from your consumer account on time or in the correct amount according to our agreement with you, we will be liable. Our sole responsibility for an error in a transfer will be to correct the error. You agree that neither we nor the service providers shall be responsible for any loss or property damage, whether caused by the equipment, software, Meezan Bank, or by Online browser providers such as Goolge Chrome and Microsoft (Microsoft Internet Explorer browser), or by Internet access providers or by online service providers or by an agent or subcontractor of any of the foregoing.

Neither we nor the service providers will be responsible for any direct, indirect, special or consequential economic, or other damages arising in any way out of the installation, download, use, or maintenance of the equipment, software, the Meezan Bank Internet Banking/Mobile App services or Internet Browser or access software. In this regard, although we have taken measures to provide security for communications from you to us via the Meezan Bank Internet Banking/Mobile App Services and may have referred to such communication as "secured," we cannot and do not provide any warranty or guarantee of such security. In states that do not allow the exclusions or limitation of such damages, our liability is limited to the extent permitted by applicable law.

Additionally, Meezan Bank will not be liable for the following:

a. If, through no fault of ours, you do not have enough money in your account to complete a transaction, your account is inactive or closed, or the transaction amount would exceed the credit limit.

b. If you used the wrong Login ID and passcode or you have not properly followed any applicable computer, Internet, or Any Bank user instructions for making transfer and bill payment transactions.

c. If your computer/Phone fails or malfunctions or the Internet Banking/Mobile App service was not properly working and such problem was or should have been apparent when you attempted such transaction

d. If, through no fault of ours, a bill payment or funds transfer transaction does not reach a particular creditor and a fee, penalty, or interest is assessed against you.

e. If circumstances beyond our control (such as fire, flood, telecommunications outages or strikes, equipment or power failure) prevent the transaction.

f. If the funds in your account are subject to legal process or other claim, or if your account is frozen because of a delinquent loan, overdrawn account, or suspected fraud.

g. If the error was caused by a system beyond Meezan Bank's control such as a telecommunications system, or Internet service provider.

h. If you have not given Meezan Bank complete, correct, or current information so Security Bank can process a transaction.

Billing Errors. In case of errors or questions about your Internet Banking/Mobile App transactions, telephone us at the phone number or write us at the address set forth above as soon as you can. We must hear from you no later than sixty (60) days after we sent the first statement on which the problem appears.

a. Tell us your name and account number.

b. Describe the transaction you are unsure about, including the transaction confirmation or reference number if applicable, and explain as clearly as you can why you believe it is an error or why you need more information.

c. Tell us the rupee amount of the suspected error.

Meezan Bank will never contact any customer and request electronic banking credentials. If you get a call asking for your credentials, hang up and call us!

Tips to Reduce the Risk in Internet Banking?

Block cookies on your Web browser: When you surf, hundreds of data points are being collected by the sites you visit. These data get mashed together to form an integral part of your "digital profile," which is then sold without your consent to companies around the world. By blocking cookies, you'll prevent some of the data collection about you. Yes, you'll have to enter passwords more often, but it's a smarter way to surf.

Don't put your full birth date on your social-networking profiles: Identity thieves use birth dates as cornerstones of their craft.

Use multiple usernames and passwords: Keep your usernames and passwords for social networks, online banking, email, and online shopping all separate. Having distinct passwords is not enough nowadays: if you have the same username across different Web sites, your entire romantic, personal, professional, and e-commerce life can be mapped and re-created with some simple algorithms. It's happened before.

Internet Banking/Mobile Problems, Concerns, or something doesn't look right? Call us at 111-331-331

Meezan Bank Digital Account Biometric Verification Data policy.

- Meezan Bank does not save/store/share any fingerprint images/data. The captured fingerprints are directly passed to NADRA (National Database and Registration Authority) APIs in the form of accepted fingerprint templates for verification of fingerprints against the citizen number.
- The current geo-location (longitude and latitude) of the user is captured at the time of biometrics verification as per the mandated by State Bank of Pakistan https://www.sbp.org.pk/bprd/2021/C2-Annex-A.pdf.