Standard Form of Agreement

Infrastructure as a Service

The Agreement

The Parties

Pakistan Mobile Communications Limited a company duly incorporated and registered under the Companies Ordinance 1984 and having its registered office at DHQ-1 F-8 Markaz Kohistan Road , Islamabad, Pakistan (hereinafter referred to as the "**PMCL**", "us", "our") and the Customer, (being an entity subscribing to PMCL for the provision of Cloud services) agree that by accessing PMCL cloud services, you (hereinafter referred to as "The Customer", "you" and "your") accept, without limitation or qualification, the terms and conditions contained within the Standard Form of Agreement.

What is the Standard Form of Agreement?

The PMCL Standard Form of Agreement (SFOA) sets out the standard terms and conditions of our services and the products we offer. The SOFA is made up of:

a) General Terms and Conditions
b) Service Level Agreement
c) Self Service Portal Pricing Schedule or Executed Proposal (If any)
d) Annexures

The Customer agrees to be bound by the SFOA as executed by PMCL and the Customer on commencement of the Agreement.

Changes to the SFOA

PMCL may change the SFOA at any time. We will notify if we change the SFOA in a way which materially impacts the Customer's use of Cloud Services, using the means detailed in Notices section.

Where we change the SFOA and notify the Customer, The Customer's continued use of the Service signifies the acceptance of the updated SFOA.

Customer Rights

PMCL offers services to the Customer on the terms and conditions of a "Standard Form of Agreement".
The Customer intends to procure from PMCL one or more of the Cloud Services in accordance with the terms and conditions of the SFOA.

Definitions

"Agreement" means this agreement for the provision of the Goods and Services by PMCL to the Customer, which includes this Standard Form of Agreement, the Service Descriptions and Self-Service-Portal Pricing Schedule.

"Business Day" means Monday to Friday excluding public holidays in Pakistan.

"Business Hours" means 9AM to 6PM every business day.

"Charges" means the charges payable by the Customer to PMCL for the Goods and Services as specified on the Self-Service Portal Pricing Schedule, Quotes or other means.

"Contract Term" means, in respect of a Service, the contract period specified in the Service Description for that Service.

"Customer Data" means all data that is not PMCL Data. Specifically, data or intellectual property that is owned by The Customer and transferred into PMCL for the purposes of using the PMCL service.

"Early Termination Fee" means the Charges that are specified as "Early Termination Fee" in the Self-Service Pricing Schedule or Executed Proposal (if any).

"Goods" means any goods we supply to the Customer, including goods supplied in connection with any Services.

"GST" means Goods and Services Tax.

“Resubmission Payment” means the fee payable to a payment processor (typically a credit card gateway or bank) when payment for a service fails.

“Self-Service Portal” means the portal that will be available for the customer to view available goods and services, make order and payments and request for support.

“Support” means assistance provided by PMCL to the Customer.

"Support Hours" means 24 hours per day, seven days per week.

"Services" means the list of services specified on the Self-Service Portal.

"Scheduled Maintenance" means maintenance carried out by PMCL where notice has been provided to the Customer by email or by posting a notice on the PMCL website prior to the scheduled event occurring.

"Standard Form of Agreement" means this document entitled “Standard Form of Agreement” and includes our Policies.

"Order" means each Order completed by the Customer (online on our Self-Service Portal) requesting the Services.

Use and Provisioning of the Customer Service

Upon our acceptance of the Customer’ Order, and execution of this SFOA by PMCL and the Customer, a contract is formed, and the Customer shall be bound by this SFOA and the terms and charges associated with the Service. The relationship between PMCL remains in force until it is terminated in accordance with this SFOA.

Customer agrees that, if Customer uses online payment option and provides incorrect information or which is actioned by a third party, Customer will be liable for a resubmission payment to PMCL.

Customer must provide true, current, accurate and complete information as prompted by the registration form. The Customer agrees to keep this information up to date.

The Customer shall be responsible for all acts or omissions that occur under Customer’s account or password, including content of transmissions through Services and maintaining confidentiality of Customer’s password/s.

Customer will operate in compliance with provisions of all applicable laws (including the laws of PAKISTAN, and in accordance with public order and Pakistan Electronic Crimes Act 2016.

Customer shall remain responsible for any access and use of the Service by its Users, all Charges incurred and compliance with all terms and conditions by it and its Users under this SFOA

Customer shall not publish, distribute or disseminate obscene, defamatory or otherwise unlawful material using the Service.

Customer shall not use the Services to threaten, harass, stalk, abuse, or otherwise violate legal rights (including rights of privacy) of others

Customer shall not use the Service to infringe on any third party's copyright, patent, trademark, trade secret or other proprietary rights or rights of publicity or privacy.

Customer shall be responsible for their Services usage and shall not use the Services nor allow the Services to be used for any unlawful or illegal purposes.

Customer acknowledges that it is their sole responsibility to comply with any rules imposed by any third party whose content or service is required to access or use the Services.

Customer shall, at all times, cooperate with PMCL's reasonable investigation of outages, security problems, any suspected breach of the SFOA and misuse of the Services.

Secure Usage

In addition to foregoing obligations, Customer is solely responsible for taking steps to maintain appropriate security, protection and backup of Customer Data. PMCL's security obligations with respect to Customer Data are limited to that which would naturally apply to the scope subscribed for. PMCL makes no other representation regarding the security of Customer Data. Customer is solely responsible for determining suitability of Services in light of the type of Customer Data used with Services.

The Customer shall use reasonable security precautions in connection with their use of the Services, including encrypting any passwords transmitted to and from, and while stored on, the Services (including the underlying servers and devices)

Unauthorised usage of Customer's Service by a third party will result in Customer being responsible for the charges incurred.

Unauthorised Usage

Any attempt to access or modify unauthorised computer system information or to interfere with normal system operations, whether on PMCL equipment or any computer system or network that is accessed by our services, may result in suspension or termination of the Customers Service. Unauthorised activities include, but are not limited to, guessing or using passwords other than Customer's own, accessing information that does not have public permission, and accessing any system on which Customer is not welcome/permitted.

Any attempt to disrupt or interfere with users, services or equipment, may result in termination or suspension of the Customer's Service. Disruptions include, but are not limited to, distribution of unsolicited advertising or spamming, monopolisation of services, propagation of, or transmission of information or software which contains, computer worms, trojan horses, viruses or other harmful components, using the network to make unauthorised entry to any other machine accessible via our network, sending harassing or threatening e-mail and forgery or attempted forgery of e-mail messages.

Software

All software provided for Customer use is subject to the terms of this SFOA. The Customer shall not remove, modify or obscure any copyright, trademark or other proprietary rights notices that appear on any software PMCL provides. Unless permitted by the terms of an open source software license, Customer may not reverse engineer, decompile or disassemble any software PMCL provides except and to the extent that the Customer is expressly permitted by applicable law to do this, and upon prior written consent of PMCL**.**

If Customer uses any non-PMCL provided software on Customer hosted system, the Customer represents and warrants to PMCL that it has the legal right to use such software in that manner. The Customer has a written license agreement with the software vendor that permits PMCL to perform installation, patching or management activities. If required information is not provided PMCL may, in its sole discretion, suspend or terminate the SFOA.

Service Cancellation

The Customer can cancel their Service via PMCL self-service portal at any time (if entitled as per respective service agreement form).

When a service cancellation is requested, we will cancel the service at the end of the billing period in which the request is received.

Service Termination

Without limiting the generality of any other clause in this SFOA, PMCL may terminate Customer's Service immediately by notice in writing if:

a) The Customer has provided PMCL with false or misleading information or the Customer has not provided PMCL with any information that we have reasonably requested for the purposes of this Agreement;

b) The Customer's nominated payment method is refused or dishonoured, or the Customer fails to pay the amount specified within fourteen (14) days of the due date.

c) The Customer is unlawfully using the Service.

d) The Customer has breached any provision of the SFOA

e) It is required under any regulatory or emergency

f) The operations, security or efficiency of a Service is impaired by Customer's use of Service or Customer Equipment connected to the Service

Customer is entitled to terminate the Service(if entitled as per respective service agreement form) at any time by giving a minimum of 60 day's prior written notice to PMCL.

Upon the Customer providing notice of termination for the respective Service, all Charges including any unbilled amounts shall become immediately payable. Customer shall be billed for all Charges up to and including the last day of the notice period (i.e. the date on which the respective Service is terminated).

Scheduled Maintenance

PMCL will endeavour to conduct all Scheduled Maintenance outside of Business Hours. However, PMCL may be required to suspend supply of Service during Business Hours in order to carry out emergency repairs on its systems.

Fault Reporting & Resolution

Customers may report service faults via Self-Service Portal "support tab" insert link. The support team will use best efforts to identify and resolve the fault.

It is Customer's responsibility to maintain and repair any equipment which Customer owns. The Customer is also responsible for any of PMCL's equipment on Customer's premises and Customer shall indemnify PMCL for any loss or damage to PMCL equipment

Service Level Agreement

Where the Service is unavailable due to scheduled Systems Maintenance, such period shall be exempted from assessment.

Where Service is unavailable due to events beyond our control, such disruption period shall be exempted. These include the following events:

a) Interruption of Service due to any Force Majeure events including any emergency or regulatory situation;

b) Interruption of Service due to Customer's applications, equipment, or facilities;

c) Where Customer causes an interruption to Service due to Customer's acts or omissions, or any use of Service authorised by the Customer;

Support Services

Services include Support during commissioning and general use of the Services.

Our Support does not extend to administration of the Virtual Machine operating system or applications contained therein unless you have purchased an explicit managed service contract.

Additional Support may be provided, although it may be at an additional cost to the Customer if the reported problem is due to faults in Customer's software, operating systems or applications.

In event of an unscheduled outage or incident, we will communicate the details of issues and expected resolution times via our website.

Our standard response time to any support issue raised is 8 business hours. In the event of a Severity 1 incident, response time is 30 minutes.

We shall not provide free support for:

a) faults that are outside our system; or
b) Customers that do not have an existing active subscription with us.

Data and Intellectual Property

Data Ownership and Responsivity

At all times, "Customer Data" remains the exclusive property and responsibility of Customer.

Customer Data Protection

Customer Data Protection: In addition to the foregoing obligations, the Customer acknowledges that they are, solely responsible for taking steps to maintain appropriate security, protection for Customer login credentials used to access the Customer Data. PMCL's security obligations with respect to Customer Data are limited to that which would naturally apply to the scope as subscribed on Self Service Portal or Executed proposal (If any). PMCL makes no other representation regarding the security of Customer Data. Customer is solely responsible for determining the suitability of the Services considering the type of Customer Data used with the Services. The Customer must maintain the security of their login credentials and may not share login credentials except as required to establish and authorise users in their account. The Customer is responsible for designating authorized users under their account and limiting access of login credentials associated with their account.

Data Retention

Once Customer cancels a Service, Customer Data pertaining to that Service shall not be retrievable form such point by the Customer in any shape or form.

PMCL may erase/delete Customer Data from our systems no later than 90 days from the date of Service cancellation.

Data Backup

PMCL does not backup Customer Data unless Customer purchases PMCL's Backup service.

Intellectual Property

Ownership of and all Intellectual Property Rights generated or for PMCL in connection with this SFOA, shall remain the property of PMCL or its licensors.

PMCL will grant the Customer a personal, non-transferable and non-exclusive license to use and to permit its Users to use, in object code form, all software and associated written and electronic documentation and data furnished by PMCL pursuant to this SFOA (the Software), solely as necessary for receipt of Service and solely in accordance with this SFOA and the applicable written and electronic documentation. The term of any license granted by PMCL pursuant to this Clause (Intellectual Property) is co-terminus with the term for the Service with which the Software is associated.

The Customer shall not, without PMCL's prior written consent, copy or download Software and shall promptly return all tangible material relating to the Software to PMCL following termination of a Service or this SFOA whichever takes place earlier unless required under applicable law and/or regulation and unless such material is required for provision of a Service which is still being provided to Customer at the time of notification of termination of SFOA. The Customer shall not take any steps to modify the Software, or reverse assemble, reverse compile (except as permitted by applicable law) or otherwise derive a source code version of Software. Software is and will remain the sole and exclusive property of PMCL or its supplier.

Neither Party acquires any rights to other Party's patents, copyrights or other intellectual property under the SFOA except the limited rights necessary to perform its obligations under the SFOA.

Customer shall not use PMCL's logo or trademark or powered by PMCL Cloud unless a written / email approval is granted via respective account manager

PMCL Equipment

Unless provided otherwise, PMCL Equipment made available to Customer as part of a Service must be returned to PMCL when the Service ends either due to completion of service term or due to termination, cancelation or nullification. If the Customer fails to return PMCL equipment in accordance with this Clause ("PMCL Equipment"), PMCL may charge Customer for non-return of PMCL Equipment.

Customer shall bear the risk of loss or damage (other than ordinary wear and tear) to provided PMCL Equipment and shall fully insure the PMCL Equipment for risk of loss, theft, destruction, and damage. Customer will be charged for any misuse, neglect and damage made to PMCL's equipment by the Customer.

Billing and Payments

Billing

PMCL may bill the Customer for:

a) recurring or fixed charges in advance;

b) variable charges, in arrears, including but not limited to excess resources, internet speed and license usage charges;

c) installation or set-up charges, before installation occurs or decommissioning charges; or

d) any equipment the Customer purchases from us, on or after delivery;

Bills may include charges from previous billing periods where these have not been remitted

Early termination Charges: If a Service that is subject to a committed term is terminated prior to expiry of committed term by the Customer (or by PMCL due to the Customer's breach of the Agreement), PMCL shall be entitled to charge early termination Charges, which shall include the difference between the yearly and monthly rental Charge for each month of Service rendered during the committed term; and an additional Charge of one month's rental, and unless otherwise stated, PMCL will not refund any Charges paid in advance for the committed term

Stolen Credit Card / Payment

Since the Customer can pay online via credit card / jazz cash / IBFT, any illegal use of payment mechanism or use of stolen / theft card by the Customer shall be sole responsibility of the Customer.

Disputed Bills

In the event Customer disputes in good faith any portion of PMCL's invoice, Customer must pay the undisputed portion of the bill and submit a written claim for the disputed amount, documenting the basis of its claim. All claims must be submitted to Service Provider as soon as is reasonably possible for such Services.

Payments

Any charges must be paid to PMCL as per the due date mentioned on the invoice.

The Customer will ensure that its billing address and payment information provided to PMCL remains current at all times.

If the Customer does not pay all of the Charges when due, PMCL may, after giving thirty (30) days written notice:

a) Suspend the usage of the Service either in whole or in relation to any specific part of the Service;

b) charge a late payment or Service restoration charge;

c) take any other debt recovery action as PMCL deems appropriate; and/or

d) terminate all or part of the Service and/or the Agreement

Taxes

All payments by the customers to PMCL shall be inclusive of sales tax (if any and as applicable). Payment will be made to PMCL after deduction of applicable withholding taxes as applicable under law. No withholding tax deduction shall be made in case if PMCL will provide valid income tax exemption certificate. In case of deduction, PMCL would be provided withholding tax certificate within 30 days of the deduction on payment.

Warranties

PMCL make no warranties that Services will meet the Customer's requirements, or that Services will be uninterrupted, secure, or error free, or the results that may be obtained from the use of Services, or to the accuracy or reliability of any communication or transmission of data, or the accuracy of any information obtained through Services or that defects in the software used to provide the Service will be corrected.

PMCL make no warranty regarding any Services or any transaction entered into through Services. We take no responsibility for deletion or failure to backup Customer Data. No advice or information, whether oral or written, obtained by Customer from PMCL or through Services shall create any warranty by PMCL.

Indemnification

The Customer agrees to fully indemnify PMCL from any claim or demand, arising out of the Service, including any violation of this Agreement by the Customer or any other person using the Customer's account, except that the Customer shall not be held liable in any way or by means for any indirect, special or consequential damages in connection with the Service, or to the extent any losses suffered by PMCL are contributed to by PMCL's acts or omissions.

CONFIDENTIALITY and ISMS

The Parties shall comply to the Confidentiality and Data Protection provisions detailed in Annex A and Annex B respectively.

The Parties shall comply to the Information Security Management System (ISMS) attached herewith as Annex C and Security requirement attached herewith as Annex IS – 02 which shall become an integral part of the Agreement.

Export Control

The Customer acknowledges that if a Service includes equipment, Software, services, technical information, training materials or other technical data which, as a result of its provenance or for other reasons, is subject to export or re-export laws and regulations of the PAKISTAN and other countries, provision of the Service may be conditional upon the prior obtaining and issuing of the approvals, authorizations and consents required by the above mentioned laws and regulations and/or upon the obtaining of said laws and regulations

Assignment and Transfers

The Customer agrees that PMCL may assign or transfer this Agreement or any of its rights or obligations under this Agreement to an Affiliate or to any successor company (whether by merger, consolidation or otherwise), or to any other person or entity at any time. PMCL shall notify the Customer of any such assignment or transfer.

The Customer Account is provided exclusively for use by Customer. Customer shall not transfer the use of Service to any third party. However, in the event a necessity arises to transfer Customer Account to any Affiliate such transfer shall be requested in writing (together with such supporting documents that PMCL may reasonably require such as a valid trade license, other corporate documentation and/or supporting financial information on the new entity). The transfer of Customer Account shall be done at the absolute discretion of PMCL. In the event of PMCL allowing the transfer of Customer Account to a new person or entity, Customer shall settle all amounts outstanding and may be required to provide an additional deposit before any such transfer.

Governing Law and Arbitration

The provisions of this Agreement and the rights and obligations hereunder shall be governed by and construed in accordance with the laws of Islamic Republic of Pakistan.

If the Parties are unable to resolve the matters in dispute relating to, arising out of or in connection with this Agreement within a period of fifteen (15) days immediately commencing from the date of original notice of the dispute(s), then all such dispute(s) shall be finally settled through arbitration by a sole arbitrator mutually appointed by the Parties, or appointed by the Court having jurisdiction in case of dispute as to the appointment of arbitrator, who shall act under the provisions of the Arbitration Act 1940. The arbitration shall be in accordance with Pakistani laws and place of arbitration shall be Islamabad - Pakistan and the language of the proceeding shall be English. The award of the arbitration shall be binding on the Parties.

CODE OF CONDUCT & Compliance Provisions:

Customer acknowledges that it has received copy of the Business Partner Code of Conduct also available at PMCL website http://jazz.com.pk/assets/uploads/pdf/BP-Code-of-Conduct.pdf (the "Code") and understands and agrees to the said Code (including all updates of the said Code made from time to time) in the course of this Agreement, including without limitation provisions with regard to anti-bribery and conflicts of interest.

The Customer understands and agrees to comply to the compliance provisions available at https://jazz.com.pk/cp-annex/.

Service Level Agreement

Support

24/7 break-fix support via Self Service Portal or email at cloud.support@jazz.com.pk

Scheduled Maintenance or a Scheduled Outage
Unavailability of the Services for the purpose of maintenance conducted by PMCL upon prior written notice.

Severity Definitions

Critical (Severity 1)
Critical production issue that severely impacts your use of the service. The situation halts your business operations and no procedural workaround exist.
Service is down or unavailable.
A critical documented feature / function is not available.

Major (Severity 2)

Major functionality is impacted, or significant performance degradation is experienced. The situation is causing a high impact to portions of your business operations and no reasonable workaround exists.

Service is operational but highly degraded performance to the point of major impact on usage.

Minor (Severity 3)

There is a partial, non-critical loss of use of the service with a medium-to-low impact on your business, but your business continues to function. Short-term workaround is available, but not scalable.

Cosmetic (Severity 4)

Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting a small number of users. Acceptable workaround available.

Response Time

Response time is defined as the duration between the time user's call is received by vendor and the time user gets the acknowledgement/ticket Number and Engineer is assigned.

Severity	Response Time
Critical (Severity 1)	30 Min
Major (Severity 2)	1 Hour
Minor (Severity 3)	4 Hours
Cosmetic (Severity 4)	8 Hours

Service Level Type

The following SLA calculation methodology will apply:

The SLA applies to the aggregate number of minutes that the active VM is available, up to the hypervisor level (OS, Application, Data Base are excluded from this SLA).
The SLA percentage for each VM (excluding OS, Data Base and Application) is 99.5% in calendar year.

SLAs apply to the complete unavailability of the Service due to non-VDC factors. That is, no access to the Service through loss of host power, storage failure or complete loss of internet connectivity.

Any software failures, patches, security vulnerabilities, inconsistencies and incompatibilities which cause system instability on the VDC are not covered under the SLA. PMCL recommends that you perform a system rebuild should you experience any service issues on your virtual appliances.

Customers are responsible for snapshots, power-up, power-down, backup and restoration/rebuild of virtual appliances.

Snapshots older than 48 hours will be automatically removed. Customers requiring a longer retention period are encouraged to contact PMCL and discuss their requirements.

Exclusions

The following will be excluded from the calculation of Qualifying Outage Minutes:

Scheduled maintenance or a scheduled outage
OS and application outage
Unavailability of Jazz Cloud Portal while Virtual Machines are running
Any misconfiguration by customer on cloud portal. This includes:

Misconfiguration of VMs hardware configuration
Missing installation of VMware Tools on any VM
Misconfiguration of ESG which includes incorrect routing, firewall rules, NAT, Load balancer or DHP services.

Any event outside of PMCL's control, including but not limited to the following examples:

Periods of emergency maintenance activities.
Problems with Customer provided Content or programming errors including, but not limited to, Content installation and integration, or failure to patch and maintain any software installed on the VM.
System administration, commands, file transfers performed by Customer representatives.
Work performed at Customer request (for example technical assistance) and other activities Customer directs.

Denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders.

Labour disputes or strikes, acts of civil disobedience, acts of war, acts against parties (including carriers and PMCL’s other vendors), and other force majeure events.

Lack of availability or untimely response time of Customer to respond to incidents that require their participation for source identification and/or resolution, including meeting Customer responsibilities for any prerequisite Services.

Customer's breach of their material obligations under this Agreement.

VMs for which Customer selects "no patch" options for patch management.

Escalation Matrix

Level 1	Self Service Portal cloud.support@jazz.com.pk 0304 111 0365
Level 2	Assigned Account Manager
Level 3	Development Expert yasim.kiani@jazz.com.pk 0307 1505041 Solution Architect- shahryar.ali@jazz.com.pk 0307 9770984

Annex A

Confidentiality

1. The Parties acknowledge and agree that in connection with this Agreement, each Party will have access to information relating to the other Party’s or its Affiliate’s business affairs, operations, products, processes, methodologies, formulae, plans, projections, know-how, IP, market opportunities, suppliers, Agents, marketing activities, sales, software, computer and telecommunications systems, costs and prices, wage rates and records pertaining to finances and personnel (“Confidential Information”) and hereby agree not to disclose any Confidential Information to any third party and not to use any such Confidential Information for any purpose other than as strictly required for the performance of this Agreement. All such Confidential Information is and shall remain the exclusive property of the Disclosing Party and no license shall be implied to be granted with respect to such Confidential Information by reason of the other Party’s access to such Confidential Information. Where Disclosing Party means the Party to this Agreement that discloses Confidential Information, directly and Recipient means the Party to this Agreement that receives Confidential Information, directly or indirectly, from the Disclosing Party.

2. Each Party agrees to protect the Confidential Information of the other with the same standard of care and procedures used by it to protect its own Confidential Information of similar importance and by using at least a reasonable degree of care.

3. Each Party undertakes to use all precautions required to enable it to comply with all the terms of this Agreement and to ensure similar compliance of the same by its employees/ personnel.

4. Exclusions: The receiving Party shall be relieved from this obligation of confidentiality to the extent that any such information:
    a. was in the public domain at the time it was disclosed or has come in the public domain through no fault of the receiving Party;
    b. was known to the receiving Party, without restriction, at the time of disclosure;
    c. was disclosed by the receiving Party with the prior written approval of the disclosing Party;
    d. was independently known by the receiving Party without any use of the disclosing Party's Confidential Information and by employees or other agents of the receiving Party who have not had access to any of the disclosing Party's Confidential Information;
    e. becomes known to the receiving Party, without restriction, from a source other than the disclosing Party.

5. The Parties agree that the terms and conditions of this Agreement shall be treated as Confidential Information and that no reference to the terms and conditions of this Agreement or to activities pertaining thereto can be made in any form without the prior written consent of the other Party. Provided, however, that

the general existence of this Agreement shall not be treated as Confidential Information. Further, either Party may disclose the terms and conditions of this Agreement:

a) if required by any Court or other governmental/ regulatory body;
b) if otherwise required by law;
c) to its legal counsel/ arbitrators;
d) in confidence, to accountants, banks, proposed investors or alliance partners and financing sources and their advisors;
e) in confidence, in connection with the enforcement of this Agreement or rights under this Agreement;
f) in confidence, in connection with a merger or acquisition or proposed merger or acquisition, or the like.

6. Upon written request of the disclosing Party at any time during the Extended Term or upon termination, the receiving Party must, at the option of the disclosing Party:
   i. promptly return all Confidential Information (or the part thereof required in such request) (including copies) to the disclosing Party in a format and on media reasonably requested by the disclosing Party;
   ii. destroy that Confidential Information (including copies) in manner specified by the disclosing Party (other than such copies required to be kept by the receiving Party by law) and promptly certify to the disclosing Party in writing that it has done so;

7. Provided, however, that the receiving Party may retain, in the sole custody of its legal counsel with the written consent of disclosing party, certain categories of Confidential Information identified to the requesting Party and which are reasonably necessary to substantiate compliance with this Agreement or otherwise required for financial, operational or auditing purposes. Any such items will remain subject to the confidentiality obligations of this Agreement. When such retained information is no longer reasonably required, it shall be, according to the instruction received in that regard, either returned to the requesting Party or be destroyed; with written certification thereof being given to the requesting Party.

8. The Parties agree and acknowledge that a breach of any of the provisions of this clause by either Party shall be deemed to be a material breach of the terms of this Agreement by that Party. In case of any breach or leakage of Confidential Information, either party shall inform of other party’s Information Security personnel or Point of Contact (PoC), within forty-eight (48) hours. In case damages caused due to leakage or breach of Confidential Information, either party shall be able to take appropriate action as per applicable law. Where Applicable Law means all applicable laws, legislation, ordinances, rules, regulations, statutes, orders, statutory instruments, edicts, bye-law and collective (labor) agreements, having force of law, including all applicable directions, codes of conduct, recommendations, guidelines, decisions or guidance from government, governmental agencies or regulators, in each case whether local, national, international or otherwise existing from time to time, and as the same may be amended or replaced from time to time of the Territory;

9. A formal procedure shall be in place for incident management and both parties shall identify their PoCs to resolve breaches / incidents but not limited of internal and external cyber-attacks.

10. The provisions of this clause relating to confidentially shall survive for three (03)

years from the termination/expiry of this Agreement.

Annex B

Data Protection

Both Parties shall take all necessary steps to ensure that they comply with license obligations, regulatory requirements, and Applicable Laws. Where 'Applicable Laws' means all applicable laws, legislation, ordinances, rules, regulations, statutes, orders, statutory instruments, edicts, byelaws and collective (labour) agreements, having force of law, including all applicable directions, codes of conduct, recommendations, guidelines, decisions or guidance from government, governmental agencies or regulators, in each case whether local, national, international or otherwise existing from time to time, and as the same may be amended or replaced from time to time.

2. Both Parties shall take all necessary steps not to cause or any of its Affiliates to breach license obligations, regulatory requirements and applicable laws and provide all necessary assistance and cooperation as is required by each Party and its Affiliates in order to maintain such compliance.

3. With respect to Data Controller (Party that controls and owns the data) and Data Processor (Party that process data) Personnel, Data Processor warrants, represents, and undertakes that it shall provide all necessary information to and obtain all necessary specific and informed consents in writing from Data Controller in order to ensure that:

(a) Both Parties can comply with its obligations to provide information to its Affiliates and any third party under the terms of the Agreement; and

(b) the processing of the Personal Information of Data Controller Personnel and their Customers as provided for in the Agreement is compliant with the applicable law. Where 'Personal Information' means data or Information extracted from data/information or Personal Information which (in each case) relates to Data Controller's Personnel, Data Controller's customers and/or any other person connected with the Data Controller and in respect of which the Applicable Laws apply, and includes traffic data;

4. Data Processor warrants, represents, and undertake that they:

(a) have and will maintain all necessary registrations and notifications to Regulators responsible for regulating compliance with license obligations, regulatory requirements, and applicable laws;

(b) have and will maintain all necessary registrations and notifications to Regulators and government agencies responsible for security compliance in each country in which Services are provided;

(c) will only process Personal Information in accordance with the Agreement. In the event that a legal requirement prevents Data Processor from complying with regulatory authority's instructions or requires Data Processor to process Personal Information other than in accordance with the foregoing sentence, Data Processor shall, unless such legal requirement prohibits it from doing so, promptly inform Data Controller of the relevant legal requirement before carrying out further processing activities;

(d) will not acquire any rights or interest in Personal Information (except for the limited licence granted under the Agreement);

(e) will maintain proper records of the processing of Personal Information, including details of any processing by its Personnel;

(f) will amend, update, delete or supplement any Personal Information forthwith if Data Controller so requests in order to comply with Applicable Law;

(g) will ensure that all Personnel involved in the delivery of Services are fully trained on their obligations under Applicable Law; and

5. Both Parties will implement appropriate technical and organisational measures against unauthorised or unlawful processing of Personal Information and against any accidental loss, destruction of or damages to Personal Information, including (without limitation) by:

(h) taking reasonable steps to ensure the reliability of any Personnel who have access to the Personal Information;

(i) ensuring a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage and appropriate to the nature of the Personal Information;

(j) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(k) ensuring the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident; and

(l) maintaining a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6. Without affecting its general security obligations, Data Processor will notify Data Controller of any changes that it wishes to implement to its organisational security measures that may affect Personal Information and shall not make such changes if Data Controller determines that such measures will or are reasonably likely to cause a breach of Applicable Law.

7. In the event of a Data Breach, each Party will:

(m) immediately notify the affecting Party in writing;

(n) take all steps to mitigate or avoid such Data Breach; and

Where 'Data Breach' means a breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration or disclosure of, or access to, Customer Personal Information.

8. Both Parties will not publish, disclose or divulge any of the Personal Information to any third party, nor allow any third party to process the Personal Information on their behalf, unless Data Controller has given its prior written consent. Where Data Collector gives such written consent and Data Processor allows a third party to process the Personal Information, Data Processor shall ensure that the third party only processes such data in accordance with the scope of the consent given by Data Controller and that

the third party is bound by the same written data protection obligations that Data Controller is subject to under this section.

9. Each Party will promptly (and within not more than 48 hours of the correspondence being received) provide other Party with notice of, and provide full co-operation and assistance in relation to:

(o) any complaint, request or enquiry made in connection with a data subject's rights in respect of their Personal Information; and

(p) any queries, complaints and other correspondence with any Regulator in relation to the processing of the Personal Information;

(q) and Data Processor will respond to any of the foregoing correspondence only after consultation with, and in accordance with the instructions of Data Controller.

10. Without prejudice to above clause, Data Processor will in a timely manner comply with, and support Data Controller to comply with, requests by data subjects to exercise their rights in respect of their Personal Information (including subject access requests).

11. On termination of the Agreement, Data Processor shall cease to use or process any Personal Information received from Data Controller under the Agreement and shall return on demand or, at the request of Data Controller, shall destroy or permanently erase all Personal Information in its possession.

12.1 As directed by the regulatory authority from time to time, both Parties shall ensure confidentiality and privacy of customer's information and to protect customers' data from being disclosed to unauthorized persons and third parties, including to Data Processor's subsidiaries, affiliates and associated companies.

12.2 Both Parties shall comply with any license obligations communicated to it by the regulatory authority from time to time.

12.3 In addition to above, Data Processor is also obligated to ensure confidentiality and protection of privacy of its customers' information under the provisions of, inter alia, following laws/regulations, including various Standard Operating Procedures (SOPs)/Instructions issued by the Regulator/Government from time to time:

- The Prevention of Electronic Crimes Act, 2016
- The Investigation for Fair Trial Act, 2013
- The Subscribers Antecedents Verification Regulations, 2015
- The Mobile Number Portability Regulations,2005
- The Protection from SPAM, Unsolicited fraudulent and obnoxious communication Regulations, 2009

Annex C

PMCL Information Security Management System Policy Manual for Suppliers

1

Introduction and Purpose

Pakistan Mobile Communications Limited (PMCL), also known as Mobilink, is a leading telecommunications service provider in Pakistan and a subsidiary of Veon Ltd.

Through a comprehensive set of information security control objectives and policy statements, this manual explains how ISO 27001 applies within PMCL. The purpose of this Policy is to outline the responsibilities of PMCL to ensure its information assets are sufficiently protected against misuse and harm by PMCL's users and its candidates for employment.

Scope

The scope of this document covers a set of directives required to be in place to support the implementation of information security in accordance with ISO 27001:2013 standard and business requirement to achieve PMCL goals for the protection and management of PMCL information assets.

All Users including employees of PMCL, contractors and authorized guests (i.e., staff, temporary staff, third-party contactors, affiliates and guests, etc.) shall comply with these directives and follow the appropriate and relevant procedures envisaged under or pursuant to this Policy Manual for Suppliers.

Terms and Abbreviations

In this Policy Manual for Suppliers, unless there is anything repugnant in the subject or context, the following terms and definitions shall have the below meaning assigned to them, however, in case of conflict or inconsistency, the definitions provided in ISO/IEC 27000:2014 (E) shall prevail:

- **Active Directory (AD) / Windows DCompanyin:** means a part of Active Platform based on Microsoft Technology that enables applications to find, use, and manage directory resources (such as user names, network printers, and permissions) in a distributed computing environment.
- **Admin / Super User:** means relevant Users within the IT department with unlimited access or extensive access rights in the application, on database level and/or operating system level.
- **Air-gapped:** means a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from insecure networks.
- **Asset / Risk Owner:** are generally heads of departments, sections, groups or individuals whose work is most affected by the Asset (s) required to provide their services, and are perceived by the PMCL as the ultimate decision makers when it comes to the management of the Asset(s).
- **Asset Custodian:** are individuals / third party entity in physical or logical possession of PMCL information or information asset. These Assest Custodians are also required to implement, operate, and maintain the security measures defined by information asset owners.
- **Asset:** includes anything that has value to the PMCL.
- **Availability:** means information being accessible and usable upon demand by an authorized entity.
- **Backup:** includes a copy of a file or directory on a separate storage media.
- **Black box testing:** means a method of software testing that examines the functionality of an application without peering into its internal structures or workings.

- **CEO:** Chief Executive Officer.

- **Change Management:** includes Process of controlling changes to the infrastructure or any aspect of services in a controlled manner.

- **Confidentiality:** means the safety, secrecy, protection and non disclosure of information and information assets against unintended or unauthorized access to the standards and directions provided in this Policy.

- **Cryptography:** is a method of storing and transmitting data in a particular form that only those for whom it is intended can read and process it.

- **CTO:** Chief Technology Officer.

- **Data:** includes any Information stored or processed by any information system.

- **DCompanyin Name System (DNS):** means a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network.

- **Firewalled segment:** refers to the portion of the network protected by a firewall.

- **FTP:** means File Transfer Protocol which is a standard network protocol used to transfer computer files between a client and server on a computer network.

- **FTPS:** means an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.

- **GCSC:** means Group Cyber Security Center.

- **HR Department:** means Human Resources Department.

- **HSSE:** means Health Safety Security & Environment.

- **HTTP:** means an application protocol for distributed, collaborative, hypermedia information systems.

- **HTTPS:** means a protocol for secure communication over a computer network which is widely used on the Internet.

- **IDS:** means an Intrusion Detection System which is a device or a software application that monitors a network or a system for malicious activity or policy violations.

- **Information Asset:** means piece of information or data, regardless of the format, that has value to PMCL.

- **Information Security (IS):** includes Protection of information from a wide range of threats in order to ensure business continuity, minimize business risk and maximize return on investments and business opportunities.

- **Information Security Event:** means an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be relevant to security.

- **Information Security Governance (ISG) Team:** means a group of employees in PMCL who are responsible for the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS for the defined scope and boundaries.

- **Information Security Incident:** is a Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- **Information Security Leadership (ISL):** means a group of employees in PMCL who are Responsible for providing oversight to the information security activities at the organization level and ensuring that overall PMCL Information Security plans and objectives are met.
- **Information Security Management System (ISMS) Coordinators: means** a group of employees in PMCL who are Responsible for monitoring compliance with ISMS Policies and Procedures within their respective operational units.
- **Information Security Management System (ISMS):** means set of policies and processes established by management to assess the security requirements, develop and implement controls, evaluate effectiveness of controls and implement improvements continual improvement process.
- **Integrity:** means accuracy and completeness of information.
- **Intellectual Property Rights (IPR):** means protections granted to the creators of IP, and include trademarks, copyright, patents, industrial design rights, and in some jurisdictions trade secrets.
- **Interested Party / Stakeholder:** means such person(s) or organization (s) that can affect, be affected by, or perceive themselves to be affected by, or perceive themselves to be affected by a decision or activity.
- **iOS jailbreaking:** is the removal of software restrictions imposed by iOS, Apple's operating system, on devices running it through the use of software exploits.
- **IPS:** means an Intrusion Prevention System which is a network security threat prevention technology that examines the network flow to detect and prevent vulnerability exploits.
- **ISO:** means International Organization for Standardization.
- **IS Manager:** means an employee at a managerial position responsible for managing Information Security of an organization.
- **Enterprise Support & Services (ESS):** Looks after Nationwide IT Helpdesk Support including End User Computing, IT Tier 2 Support, Unified Communication [VC] and Enterprise Security Operations & Planning.
- **LDAP:** means Lightweight Directory Access Protocol (LDAP) which is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.
- **Local Laws:** Laws applicable within Pakistan.
- **Malicious Activities:** Any activity specifically intended to cause harm to an organization or its computing resources.
- **NDA:** means Non-Disclosure Agreement.
- **NOC AMT:** means a Network Operations Center – Access Management Team, a centralized group within PMCL responsible for managing Access Management over information Asset(s).

- **Outlook Web Access (OWA):** means establishing access to Microsoft Exchange Server mailbox from almost any web browser.
- **Password:** means secret words, letters, numbers, symbols, characters, phrase or any combination thereof in electronic form that must be used to gain access/admission to the system.
- **Penetration testing:** means the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
- **PMCL Users:** Are users with access to PMCL information and information processing environment categorized into the following user groups:
  - Permanent / Contractual Staff
  - Trainees / Interns
  - Company / Third-party Service Providers
  - Guests
- **PMCL:** means Pakistan Mobile Communications Limited.
- **Policy:** Intentions and direction of PMCL as formally expressed by its Top Management pursuant to the ISMS Policy Manual (which shall be furnished upon request) or relating to or for the purposes of Information Security Management Systems
- **Procedure:** means specified and prescribed way to carry out an activity or process.
- **Public networks:** means a type of network wherein anyone, namely the general public, has access and through it can connect to other networks or the Internet.
- **Root Cause Analysis**: is a method of problem solving that tries to identify the root causes of faults or problems. A root cause is a cause that once removed from the problem fault sequence, prevents the final undesirable event from recurring.
- **Recovery:** means retrieval of data/operations/services/information/Asset (s) in case of disruption.
- **Risk Assessment:** means overall process of risk identification, risk analysis and risk evaluation.
- **Risk:** mean effect of uncertainty on objectives.
- **S/MIME:** means Secure/Multipurpose Internet Mail Extensions is a standard for public key encryption and signing of MIME data.
- **Secure Shell (SSH):** means a cryptographic network protocol for operating network services securely over an unsecured network.
- **Service Level Agreement (SLA):** means a part of a contract/agreement wherein the service provider specifies in measurable terms, what services will be furnished at the given KPIs and for achieving objectives smoothly.
- **SFTP:** means SSH File Transfer Protocol, or Secure File Transfer Protocol which is a separate protocol packaged with SSH that works in a similar way over a secure connection.
- **SLT:** means Senior Leadership Team constituted for the purpose of this Policy.
- **SOC:** means Security Operations Center.
- **Stakeholder:** means a Person(s) or organization(s) that can affect, be affected

by, or to perceive themselves to be affected by a decision or activity.

- **Static code analysis:** means a method of computer program debugging that is done by examining the code without executing the program.
- **Supplier / Third-party:** means a person(s), firm or body that is recognized as being independent from PMCL and is providing services to the PMCL under an agreement/arrangement. Examples include service providers, maintenance agencies, consultants, technology partners and trainees.
- **Teleworking:** means a work arrangement in which employees do not commute to a central place of work.
- **Telnet:** means a user command and an underlying TCP/IP protocol for accessing remote computers.
- **Third party code review:** means a software source code review performed by an independent expert.
- **Threat:** means a potential cause of an unwanted incident, which may result in harm to an IT/computing system, Asset or organization.
- **TIA-942:** means the Telecommunications Industry Association (TIA) ANSI/TIA-942-A Telecommunications Infrastructure Standard for Data Centers which is an American National Standard (ANS) that specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms including single tenant enterprise data centers and multi-tenant Internet hosting data centers.
- **Transport Layer Security (TLS):** means TLS and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network.
- **Top Management:** refers to the PMCL Information Security Leadership team.
- **UPS:** means an uninterruptible power supply, also uninterruptible power source, UPS or battery/flywheel backup which is an electrical apparatus that provides emergency power to a load when the input power source or mains power fails.
- **User Account:** A user is a person who uses a computer or Internet service. A user may have a user account that identifies the user by a username (also user name), screen name (also screen name).
- **Virtualization:** means the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources.
- **VLAN:** A virtual LAN (VLAN) is any broadcast dCompanyin that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).
- **Vulnerability:** means a weakness in a computing system that can result in harm to the system or its operations, especially when this weakness is exploited by a hostile person or organization or when it is present in conjunction with particular events or circumstances.
- **Vulnerability Analysis:** Also known as vulnerability assessment which means a process that defines, identifies, and classifies the security holes (vulnerabilities)

in a computer, network, or communications infrastructure.

- **Wireless networks:** means the computer networks that does not require to be connected by cables of any kind for its functioning.

The following activities are, in general, prohibited. Under no circumstances, a third party of PMCL is authorized to engage in any activity that is illegal under local, international law(s) and PMCL policies while utilizing PMCL owned resources. Any breach of the PMCL's Acceptable Use Policy may lead to legal action as per the agreed contractual terms.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

- PMCL's proprietary information stored on computing devices, whether owned or leased by PMCL, its employee or a third party, remain the sole property of PMCL. Hence:
  - ✓ PMCL third parties have a responsibility to promptly report the theft, loss or unauthorized disclosure of PMCL's proprietary information.
  - ✓ PMCL third parties may access, use or share PMCL's proprietary information only to the extent it is authorized and necessary to fulfil their assigned job duties / contractual obligations.
- All mobile and computing devices of third party staff that connect to the internal network must comply with all applicable PMCL policies along with PMCL's Access Control Policy.
- The installation or distribution or use of "pirated" or other software products that are not appropriately licensed for use by PMCL is strictly prohibited.
- Unauthorized copying or the installation of any copyrighted material or software for which PMCL or the end user does not have appropriate management permission and an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting official business, even if you have authorized access, is strictly prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.
- Causing security breaches or disruptions of network communication is strictly prohibited. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the Information Security Governance (ISG) is made.
- Executing any form of network monitoring which will intercept data which is not intended of the third party's job/duty is strictly prohibited.
- Introducing honeypots, honeynets, or similar technology on PMCL's network is strictly prohibited.
- Interfering with or denying service (for example, denial of service attack) is strictly prohibited.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet is strictly prohibited.
- Providing information about, or lists of, PMCL's employees to parties outside PMCL, without appropriate approval is strictly prohibited.
- The PMCL provides Internet access to third party staff to assist them in carrying out their duties for the Company. It should not be used for personal reasons.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) is strictly prohibited.

- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages is strictly prohibited.
- As such, third party staff are prohibited from revealing any PMCL confidential or proprietary information, or any other information not classified as public as per the PMCL Information Asset Classification Policy on online forums of social media.
- Third party staff shall not engage in any blogging or online posting that may harm or tarnish the image, reputation and/or goodwill of PMCL and/or any of its employees.
- PMCL's trademarks, logos and any other PMCL intellectual property may also not be used by Third party staff in connection with any personal online activity.
- Introduction of any hardware or software in PMCL environment containing backdoors is strictly prohibited
- Any activity(ies) or action(s) carried out on PMCL network or in PMCL environment shall be properly authorized by PMCL relevant and authorized personnel and be notified well in advance before carrying them out
- Bypassing or circumventing any security controls are strictly prohibited
- Compliance and sharing of filled information for the two forms namely "PMCL-LST_SR-Third Party Agreement Security Requirement - v1.0" and "PMCL-FRM_SR-Third-party Access - v1.0" shall be submitted by the supplier

PMCL-FRM_SR-Third-party Access - v1.0

PMCL-LST_SR-Third Party Agreement Sec

I/We, do hereby declare that I/We have read and fully understood the above terms and conditions, and that I had the opportunity to discuss the same with the Information Security Governance, and that I/We agree to be bound by the directives of the above terms and conditions as laid by PMCL and its representative from time to time.

Annex IS - 02

User Registration and Anti-Identity Theft and Anti-Phishing Declaration.

Identity theft is unauthorized access to personally identifying information (PII), including Critical User Information including Customer Data Records and work or personal Email or other passwords which are used to gain access to critical information. Many people associate such crimes with online scams such as phishing emails. However, most identities are stolen using low-tech methods. There are many ways thieves may obtain your personal information by using:

- **Phishing/Spam:** They send an email, Facebook or pop-up message that looks like it came from a real bank or credit card company asking for identifying information. (This is called phishing.)
- **Social engineering/pretexting:** They pose as a legitimate business or government officials to obtain your personal information or work information that can be later used to exploit at the source.
- **Shoulder surfing:** Someone watch you from a nearby location as you type in your password or other confidential information, or listen in on your telephone conversation.
- **Hacking:** Some to gain unauthorized access into computer networks where information is stored, it includes to get the access to a system that is being used to connect to a Server Machine or system that has critical information stored on it.
- **Dumpster diving or trash rips:** Rummage through communal or business trash to obtain copies of personal or critical records that typically bear critical management plans, business or personal information. If such information needs to be trashed, Trash it completely.

Thieves can use illegally obtained personal identity information, your work passwords or your personal accounts that can be used later used to gain access to the critical information / exploit the systems. Phishing is a cybercrime where well designed and legitimate looking emails and pop up messages lure victims into revealing their username, password, or other sensitive information. The Phishing messages look authentic to the kind of communication you would expect to get from the person you trust.

However, you should never trust email or pop up messages that ask you to confirm, validate, or update your information by responding to the email or by following a link. The following needs to be keenly observed to be secure:

- Never reply to any message of email that asks for your User ID, password, work account information, or anything else that would be considered sensitive information.
- Immediately report any suspicious email to your manager or your POC assigned by PMCL, or Information Security Teams at isg@mobilink.net.
- Never click on a link in a message or pop up. Never call phone numbers that are provided in messages that ask for personnel information.
- Delete suspicious messages without opening them.
- NEVER try your work Passwords on any link even if shared by your colleague or by a Facebook/Social Media User.
- BEWARE Look after the Password Safety is your personal responsibility, If your password is compromised, you are solely responsible for it.

PMCL will NEVER send a message asking you to validate, confirm, or update your personal information and passwords.

Always be suspicious of requests for personal information that come via email, Facebook, particularly requests for personal and work passwords and accounts, banking information, or wire transfers of money, even if the request seems to come from a good friend.

Prevention of Electronic Crime Act 2016 Pakistan - for whoever commits/involved or threatens to commit has non-bail-able prison of seven years or with fine up to five million rupees or both.

BEWARE – Password is your Secret, When Shared with anybody or on Portal it's no more secret and all activities from your account shall be your Sole Responsibility.