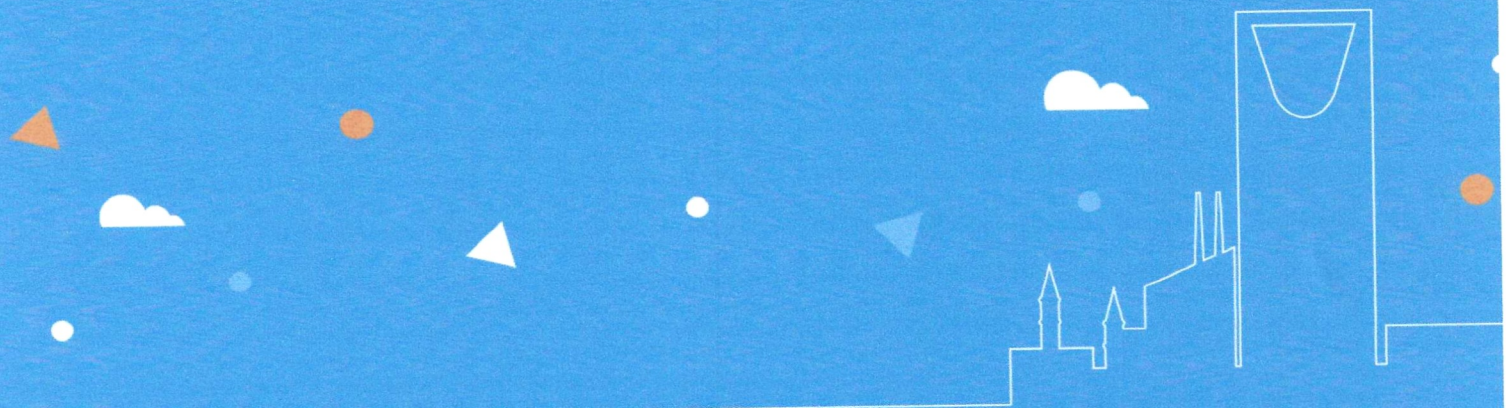




Security Measures for Handling and Protecting Client Data

Introduction:

At Taqnyat, we take the security and privacy of our clients' data very seriously. We offer a range of products and solutions such as SMS, WhatsApp Business API, emails, voice messages, live chat, and chatbots. All of the data collected from these channels is stored securely in Saudi Arabia, and we comply with the highest standards set by the Communications and Information Technology Commission (CITC) to preserve customer privacy. In this document, we will describe the measures we have taken to ensure the confidentiality, integrity, and availability of our clients' data.

Storage:

At Taqnyat, we understand the critical importance of data security and take all necessary steps to ensure that our clients' data is stored securely. We store all client data within Saudi Arabia, where we have robust security protocols in place to safeguard against unauthorized access or malicious attacks.

To ensure the confidentiality and integrity of data, we implement industry-standard measures such as encryption and access control. All data is encrypted using a strong encryption algorithm, which ensures that the data remains confidential and protected against unauthorized access or theft. Our encryption algorithm employs state-of-the-art cryptographic techniques that make it virtually impossible for hackers or other unauthorized parties to access or decrypt the data.

Furthermore, access to client data is strictly controlled and limited to authorized personnel only. We have a rigorous access control policy that ensures that only employees who require access to the data for legitimate business reasons are granted permission to access it. Access to client data is audited, and any unauthorized access attempts are immediately detected and investigated.

We also conduct regular security assessments and audits to ensure that our security protocols are up to date and effective. Our security team continuously



monitors our systems and data storage facilities to detect and prevent security breaches.

In conclusion, we take the security and privacy of our clients' data very seriously, and we are committed to providing the highest level of protection against data breaches and cyber attacks. Our industry-standard measures, robust security protocols, and regular assessments ensure that our clients' data remains safe and confidential at all times.

Access Control:

To ensure that access to client data is restricted to authorized personnel only, we implement a range of access control measures. We have a strict access control policy that defines the roles and responsibilities of employees who are granted access to client data. Access to client data is granted only to the PDA role for governmental purposes, and no other employee has access to the data.

We use strong authentication mechanisms, including two-factor authentication, to ensure that only authorized personnel can access client data. Two-factor authentication requires users to provide two forms of authentication to access the data, such as a password and a one-time code sent to their mobile device. This provides an additional layer of security to prevent unauthorized access.

We also monitor all access to client data and audit logs to detect any unauthorized access attempts. Any unauthorized access attempts are immediately detected and investigated by our security team, and appropriate measures are taken to prevent future unauthorized access.

Our access control measures are reviewed regularly and updated as needed to ensure that they remain effective against emerging threats and attacks. We continuously monitor our systems and data storage facilities to detect and prevent security breaches.



In conclusion, our access control measures are designed to ensure that only authorized personnel have access to our clients' data. We use strong authentication mechanisms, monitor all access to client data, and audit logs to detect any unauthorized access attempts. We are committed to providing the highest level of security and privacy to our clients and continuously review and update our access control measures to ensure their effectiveness..

Passwords:

we understand the importance of keeping client passwords secure and have implemented measures to ensure that passwords are stored securely. We use the MD5 hashing algorithm to store client passwords, which is considered a secure method for password storage.

MD5 is a one-way hashing algorithm that converts a password into a fixed-length string of characters, known as a hash. The MD5 algorithm is designed in such a way that it is almost impossible to reverse-engineer the password from the hash. This makes it a secure method for password storage since even if an attacker gains access to the password database, they would not be able to easily retrieve the actual password from the hash.

In addition to using MD5 to store passwords securely, we also enforce two-factor authentication (2FA) for all accounts. 2FA requires users to provide two forms of authentication to access their account, typically a password and a one-time code sent to their mobile device or email. This provides an extra layer of security, making it much more difficult for an attacker to gain access to an account even if they have managed to obtain the password.

We also have strict password policies in place that require clients to create strong, unique passwords and to change them periodically. We enforce password complexity requirements, such as minimum length, and do not allow the use of easily guessable passwords.

We take the security of our clients' passwords very seriously and are committed to using industry-standard measures to ensure that passwords are stored securely. Our password storage policy, combined with our two-factor



authentication and strict password policies, helps to ensure that our clients' accounts are well protected against unauthorized access.

In conclusion, at Taqnyat, we use MD5 to store passwords securely and enforce two-factor authentication for all accounts. We have strict password policies in place to ensure that clients create strong, unique passwords, and we continuously review and update our password storage policies to ensure their effectiveness.

Encryption:

we understand the importance of keeping customer data confidential and have implemented strong encryption mechanisms to ensure that customer data remains secure. We use a two-key approach to encrypt all customer content, which ensures that only authorized personnel can access the customer data.

To begin with, we use a strong encryption algorithm to encrypt all customer content. This encryption algorithm is designed to scramble the data in such a way that it is unreadable without the correct decryption key. This ensures that even if an attacker gains access to the encrypted data, they will not be able to read the content without the decryption key.

To further ensure the confidentiality of customer data, we use a two-key approach to encrypt the content. The first key is sent to the client via SMS, and the second key is stored on our end. The two keys are then used to encrypt the customer data in such a way that only authorized personnel can access the data.

The first key, which is sent to the client via SMS, is unique to each customer and is used to encrypt the customer content. This ensures that even if an attacker gains access to the encrypted data, they will not be able to read the content without the first key. This first key is only known to the customer, which ensures that only the customer can access their own data.



The second key, which is stored on our end, is used to further encrypt the customer data. This second key is also unique to each customer and is known only to authorized personnel within our organization. This ensures that even if an attacker gains access to the first key and the encrypted data, they will not be able to read the content without the second key.

The two-key approach to encrypting customer data ensures that only authorized personnel can access the data. In addition to this, we have strict access control measures in place to ensure that only authorized personnel have access to the customer data. Access to customer data is limited to the PDA role for governmental purposes only, and no other employee has access to the data.

We continuously review and update our encryption mechanisms to ensure that they are effective and up-to-date. We also conduct regular penetration testing and security audits to identify any vulnerabilities in our system and address them promptly.

Taqnyat's connection flow is designed to ensure seamless integration with our clients' and vendors existing systems and below diagrams explain how integration work for each product.



1. SMS connection flow between Taqnyat and Vendors

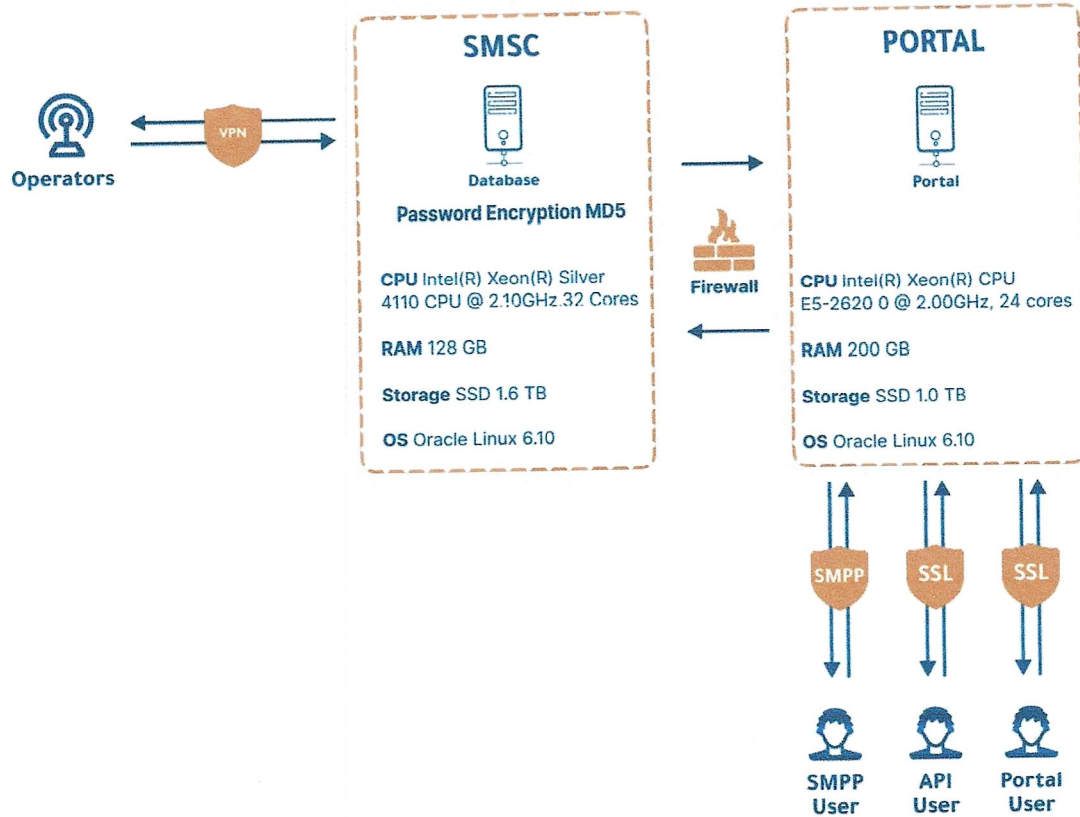
At Taqnyat, connecting with mobile operators such as STC, Zain, and Mobily is done via VPN to ensure the security of the data transmitted. The connection flow involves two servers, the SMS Center (SMSC) and the portal server. The SMSC server communicates with the operators by sending and receiving messages, while the portal server is connected to the SMSC server via a firewall.

The portal server provides clients with the ability to send SMS messages through different protocols, such as SMPP, API, or through the web portal. Each of these methods has a secure mechanism for encrypting the transfer of data to ensure that the data is protected from unauthorized access.

For instance, the API and web portal methods are secured with SSL encryption. This ensures that any data transmitted between Taqnyat's portal server and the client's device is encrypted and protected from prying eyes. The SSL encryption mechanism also ensures that the client's personal and sensitive information, such as phone numbers and message content, are kept confidential and secure.

Overall, Taqnyat's SMS connection flow is designed to ensure the security and privacy of its clients' data. By employing secure protocols and mechanisms for encrypting data, Taqnyat guarantees that its clients can confidently use their platform to send SMS messages without worrying about potential security breaches.





2. WhatsApp connection flow between Taqnyat and Vendors

At Taqnyat, we understand the importance of secure and reliable communication channels for businesses. That is why we have established a robust connection flow for WhatsApp Business API to ensure that our clients' data is always protected. We employ industry-standard safeguards that exceed regulatory requirements to ensure the confidentiality, integrity, and availability of user data.

Our WhatsApp connection flow employs a multi-layered security approach, starting with password and authentication measures. All requests to the WhatsApp API must be authorized with an API key, which ensures that only authorized personnel can access the data. Additionally, we configure the access to the WhatsApp Business API client with HTTPS, which generates a self-signed certificate by default when created. The Webhooks used in the system also require HTTPS for callbacks.

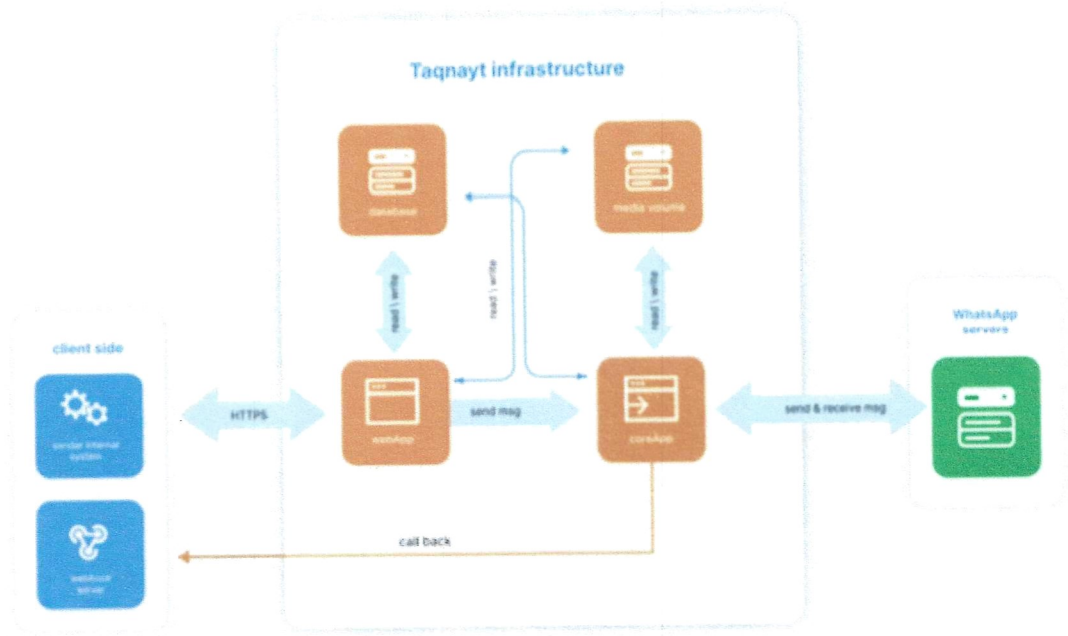
Our network segregation mechanism ensures that we host the Webapp and Core app nodes in separate, segregated networks, exposing them only to required services. This means that we limit access to the network to only necessary parties, ensuring that the data remains safe from unauthorized access.

We also ensure that all messages sent through our WhatsApp connection flow are encrypted, which means that only the authorized recipient can access the message. We have a technical whitepaper that provides an overview of our WhatsApp encryption measures for further reading.

At Taqnyat, we act as a data processor on behalf of our clients who use the WhatsApp Business API. We process data to and from the WhatsApp Business Solution according to the instructions of businesses communicated through WhatsApp API or their Integration Partner. Our clients and Taqnyat commit to compliance with all applicable privacy laws and regulations to ensure that our data processing activities are conducted in a transparent and legal manner.

In summary, our WhatsApp connection flow employs a multi-layered security approach, including password and authentication, SSL configuration, network segregation, message encryption, and data processing measures, to ensure that our clients' data is always protected.





In conclusion, at Taqnyat, we use a two-key approach to encrypt customer data, ensuring that only authorized personnel can access the data. We use a strong encryption algorithm to encrypt all customer content and have strict access control measures in place to ensure that only authorized personnel have access to the data. Our commitment to using industry-standard measures to encrypt customer data ensures that our clients' data is protected from unauthorized access and remains confidential.

Monitoring:

Monitoring is an essential aspect of any organization's security strategy to ensure the protection of their sensitive information and critical assets. The process of monitoring involves the use of various technologies and tools to identify potential security breaches and suspicious activities in real-time. By continuously monitoring their systems, organizations can quickly detect any unauthorized access attempts and take appropriate measures to prevent future attempts.

One of the primary reasons for monitoring is to detect and prevent security breaches. A security breach can be defined as any incident that results in unauthorized access, loss, theft, or corruption of an organization's sensitive information or critical assets. Security breaches can occur due to various reasons, including human errors, system vulnerabilities, or malicious attacks by external or internal actors. By monitoring their systems, organizations can quickly detect any unusual activity and investigate it before it becomes a significant security threat.

Another critical aspect of monitoring is the detection of suspicious activities. Suspicious activities can include any action that deviates from the normal behavior of users, such as unauthorized login attempts, data exfiltration, or malware infections. By detecting these activities early, organizations can take appropriate measures to mitigate the potential damage and prevent future attacks.

The process of monitoring involves the use of various technologies and tools, including intrusion detection systems (IDS), security information and event management (SIEM) systems, and log management systems. IDS is used to monitor network traffic and identify any unauthorized access attempts or suspicious activities. SIEM systems are used to correlate data from various sources and detect any security incidents in real-time. Log management systems are used to collect, store, and analyze log data from various sources, including network devices, servers, and applications.

In conclusion, monitoring is a crucial aspect of any organization's security strategy to ensure the protection of their sensitive information and critical assets. By continuously monitoring their systems, organizations can quickly detect any potential security threats and take appropriate measures to prevent them. The use of various technologies and tools can help organizations improve their monitoring capabilities and enhance their overall security posture.



Conclusion:

In conclusion, at Taqnyat, we take the security and privacy of our clients' data very seriously. We store all data securely within Saudi Arabia and comply with the highest standards set by CITC to preserve customer privacy. We employ strict access control measures and use strong encryption algorithms to ensure the confidentiality, integrity, and availability of customer data. Our systems are continuously monitored for potential security breaches, and we take appropriate action to prevent future attempts.

