

Technical Document

CraftCode AG
0798956413
Wanderstrasse 133
Basel, Switzerland
info@craftcode.ch
craftcode.ch



Table of Contents

Technical process flow description

Message flow
Message format
Fund Flow
Others

Overview of proposed infrastructure

Hardware
Software
Network Communication
Network Diagram
Bank/other institutions integration
Others

Hardware details

Value and source
Module wise functionalities
Proposed DC and DR
User capacity, TPS and session

Software Details

Value and source
Module wise functionalities
Payment Gateway Software
Proposed DC and DR
User capacity, TPS and session

Detail network plan

IT risk management process

Physical security
Data security
System rules
Access right management

Business continuity and disaster recovery plan

Settlement, reversals and dispute management process

ICT Security Policy

Data Protection Policy

Password Management

Merchant Onboard and Payment HDL

HLD

Functional Requirement Specification

Non-functional requirement specification

Software Quality Test Plan

Software Test Report

1. Technical process-flow description

The technical connection of a shop to the payment network with a payment service provider can usually be carried out with just a few clicks and requires no programming knowledge. For the majority of all popular shop systems, PSOs provide "payment modules" - in simple terms, these are plug-ins that merely need to be installed or activated in the relevant shop system. After the successful conclusion of a contract with a payment service provider, an activation takes place within a few days and business operations can begin.

1.1 Message Flow

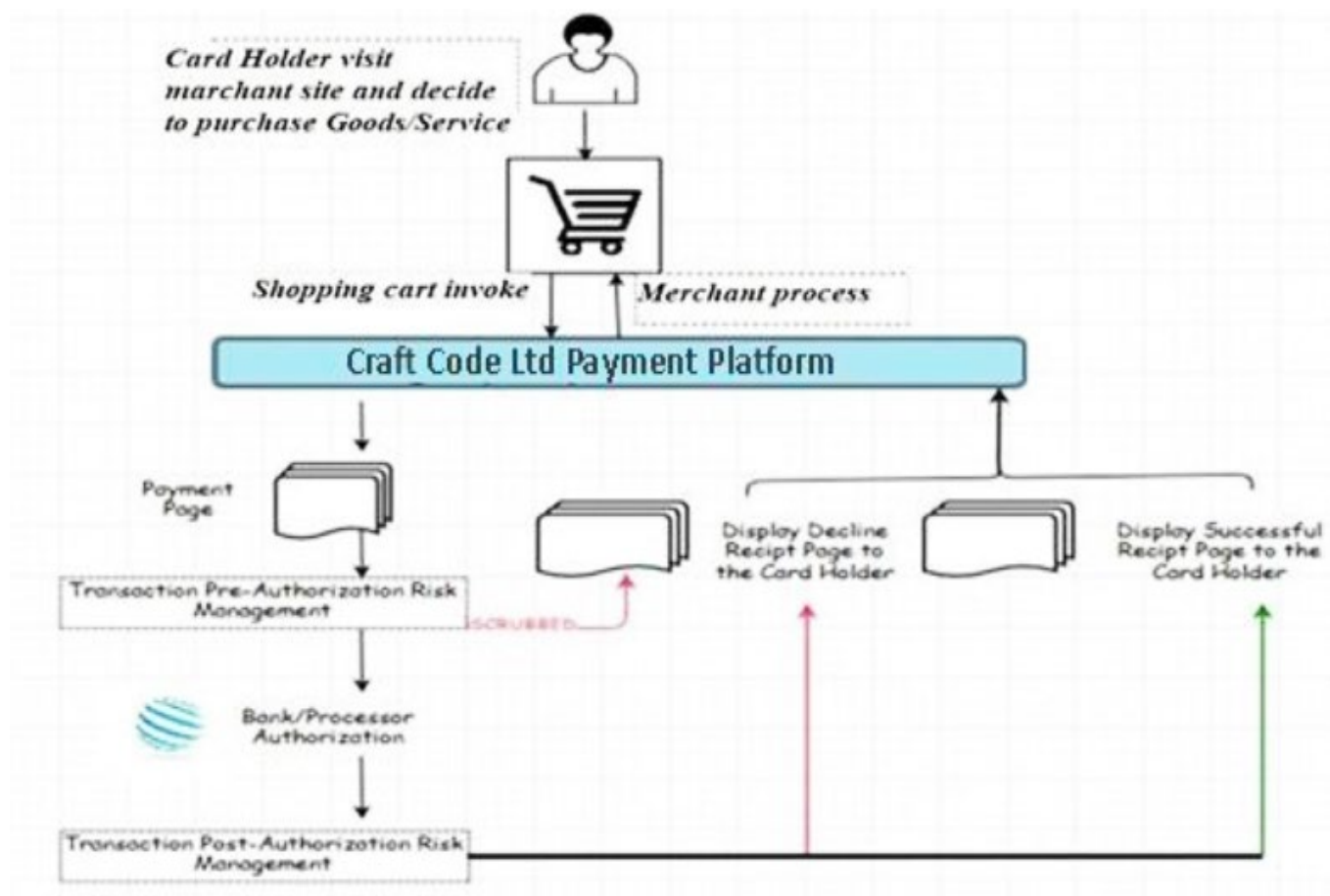


Diagram: Message Flow of Payment Gateway Platform

1.2 Message Format

Types of Message:

- Warning – General warning message, mostly client side.
- Notice – Notice for customers, mostly generated from server side.
- Approval/Validation – Any kinds of security or validation purpose, critical and important

Formats:

- Popup with no Confirmation Button
- Popup with confirmation (YES/NO) button
- In-page message
- Popup on select for real-time calculation/verification
- Standard SMS
- Standard Email

The payment information received in the gateway and sent to acquiring bank uses SSL-encrypted (256-BIT) message format. Moreover, 3D security of the transaction message is ensured by card network, acquiring and issuing bank.

1.3 Fund Flow

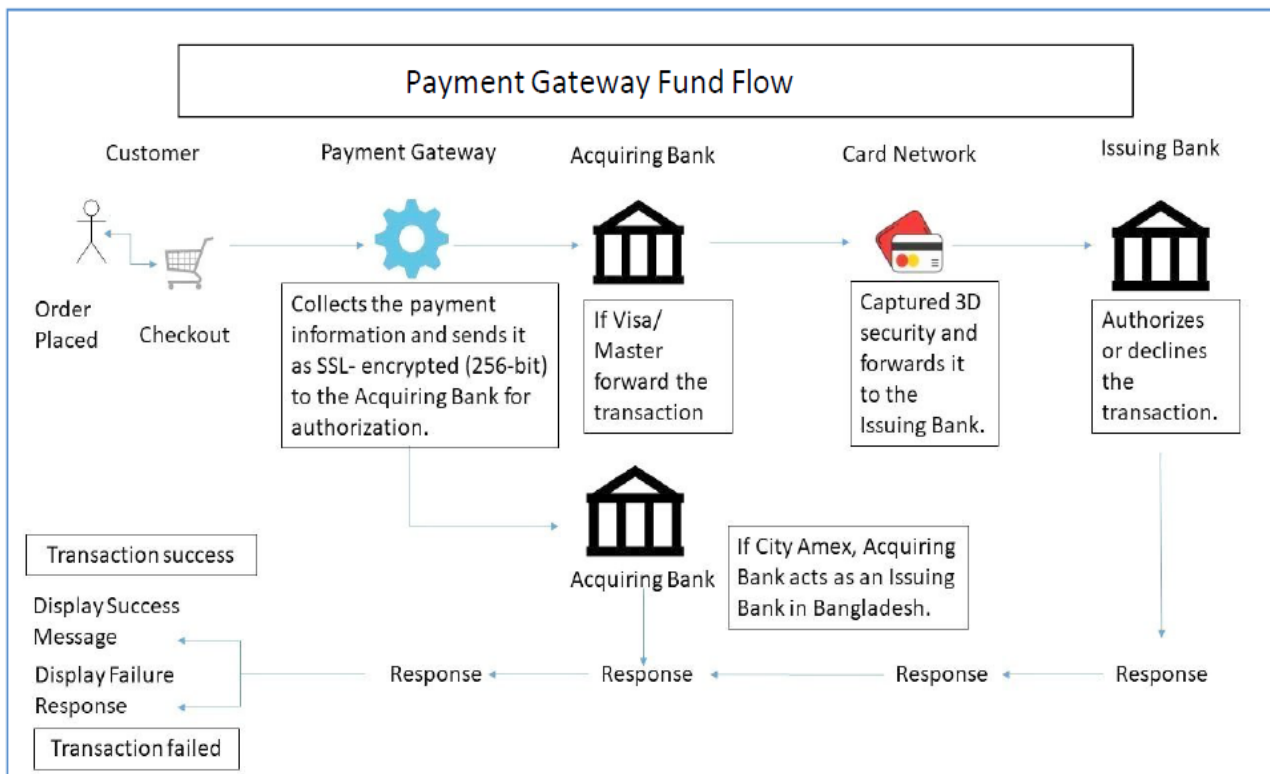


Diagram: Fund Flow of PSO

1.4. Others

Payment Service Operator

A third party that helps Merchants accept and facilitate payments. Payment Service Operator partners with **Settlement Banks** and **Issuing Banks** to offer **Merchants** the capability to accept payments. To finalize the transaction and all four stakeholders works synchronize with each other.

Here each stakeholders' activities flow describes on the basis of above diagram.

How Does a Settlement Bank Work with PSO?

The PSO enters the process during the confirmation request of the payment. After having received the request, the PSO forwards the payment information to the Settlement Bank (who will then redirect the information to the issuer). Based on the credit limit on the card and its validity, the payment will either be accepted or rejected. This confirmation/rejection is then sent back to the PSO. The PSO therefore acts as a middle-man between Settlement Bank and Merchant. The main function of the Settlement Bank consists of capturing the authorization and the processing of card payment transactions.

How Does an Issuing Bank Work?

An Issuing Bank is responsible for any card holder's ability to pay off the debt he or she accumulates with the Card or line of credit given by the bank. The Issuing Bank initially writes a letter of credit, which ensures the payment of interest and principal on any purchase made by the card holder.

2. Overview of proposed infrastructure

Payment systems are managed by payment system operators and underpin the delivery of payment services. They are effectively a set of rules that govern transfer of funds between PSPs. A further critical element of payment systems is the provision of infrastructure - essentially the various hardware, software, secure telecommunications network and operating environments that are used to manage and operate payment systems. This infrastructure supports the clearing and/or settlement of a payment or funds transfer request after it has been initiated.

2.1 Hardware and Software

To qualify as PSO our Proposed Hardware and Software fulfill the following required functions

- Accept payment from cards, or other forms of online payment
- Connect the e-commerce website to financial Institutes processes online transactions
- Encrypt sensitive information via a virtual terminal
- Securely process methods of online payment.

2.1.1 Payment service operator hosting

To become an independent payment service operator, a business can either implement its own server infrastructure or use a third party hosting (such as amazon, fire-hoster Rack-space). Local hosted server will be used by This payment gateway Plate-form for hosting.

2.1.2 Card Machines

Also known as a payment terminal, to process card transactions. Card machines will use a connection via phone or internet to transmit the transaction details for present transactions that are swiped, keyed-in or dipped in the chip card reader.

We can also connect peripherals such as PIN pads and Near-Field Communication (NFC) readers for accepting “contact less payments” such as Android or Apple Pay, although many newer machines have those built in.

2.1.3 Card Readers

These are the little card readers that will be connected with PC, smartphone or the tablet.

2.1.4 Virtual Terminals

Users can punch in the details of phone orders/mail orders via virtual terminal as long there is an internet connection. These either run as a standalone application on your computer or smartphone, or more often you just access a login URL in your web browser and process payments right in the browser window from any connected device.

2.1.5 Mobile Payment Processing

Payment Gateway going to give users the ability to process mobile payments by default.

2.1.6 Flexible customization

Payment Gateway Platform will setup and configure payment platform, to fit all your business- specific needs. Each user will get individual solution with free of charge setup.

2.1.7 Powerful fees and rates configuration

Our proposed software gives you maximum freedom in setting tariff plans for the users.

2.2 Network Communication

Following Diagram-resents a high-level view of general setup of Payment Gateway Platform. In this diagram, the thin lines represent payment information flows from providers of one type of payment service (transaction services, payment instruments and accounts, clearing services, and settlement services) to providers of the next level of services required to transfer payments. These payment information services are provided, horizontally, to each group of service providers at each service level and entail both data processing and data messaging. These are a fundamental part of the technological linkages among the various service providers in the payment transfer chain.

The thick lines represent the actual money transfer links, first between individuals and their deposit or credit accounts at their payment service operator, and possibly via currency transfers; and then between payment service operator and their settlement agents, often the banks, FIs, PSOs, on line service providers, and, in settlement networks.

The individuals originating and receiving retail payments in the system illustrated in the diagram do so through payment instruments and related services acquired from their banks or other payment service operators. They use a variety of transaction mechanisms that banks own individually or collectively or through third-party vendors that provide access to such networks.

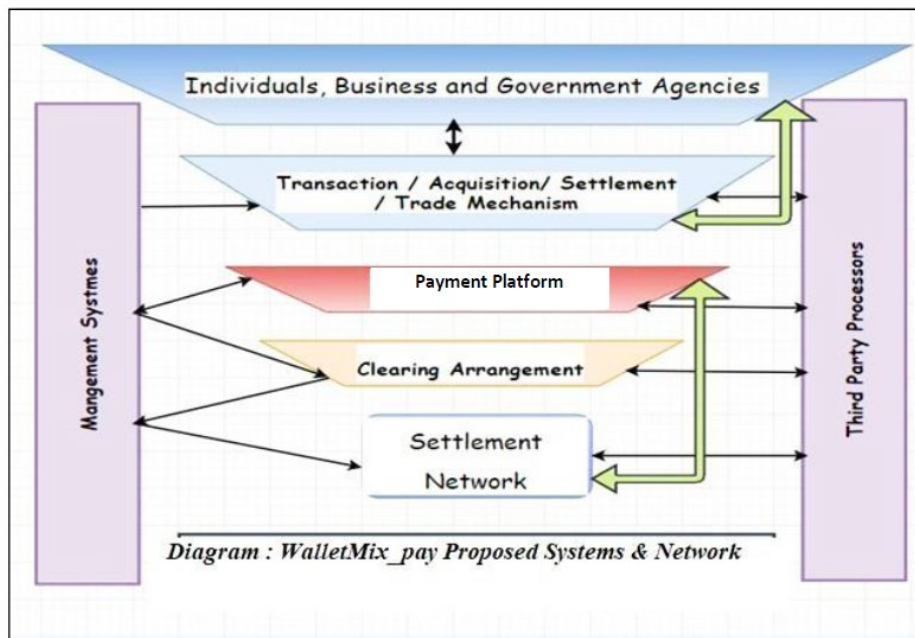
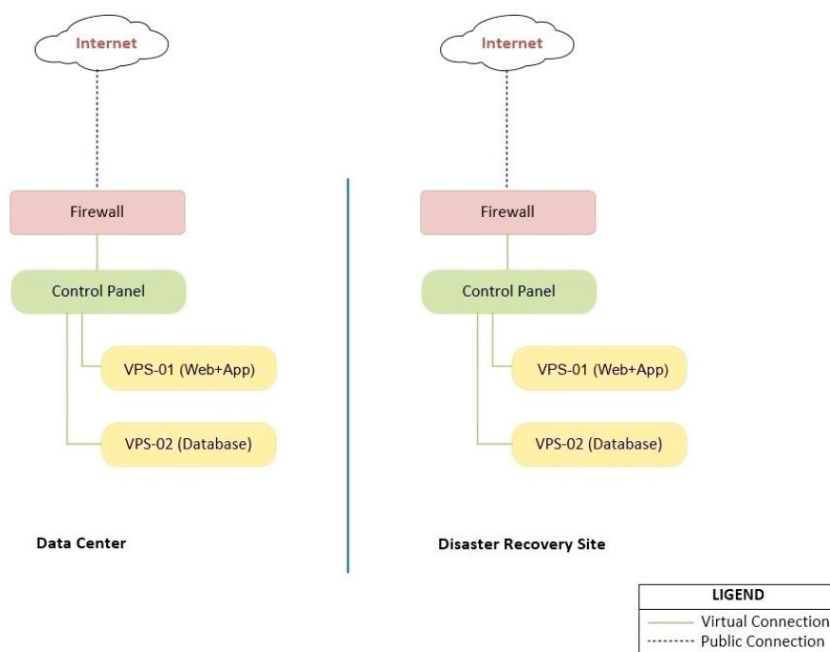


Figure: Process to become a direct settling participant



Title: Network Diagram of Craft Code Ltd Date: March 20, 2024

2.3 Bank / other institutions Integration

There will be a communication and Integration plan that has a clear overview of which stakeholders will be informed when and with what message flows among different stakeholder. The roles and responsibilities of the concerned parties (such as financial institutions, issuers, acquirers and PSOs etc.) pertaining to the processing, clearing and settlement of transactions must be governed under the relevant contracts/agreements. Transactions processed by PSOs will be settled amongst the participants at any commercial banks, FIs licensed by BB or as per the instructions by BB.

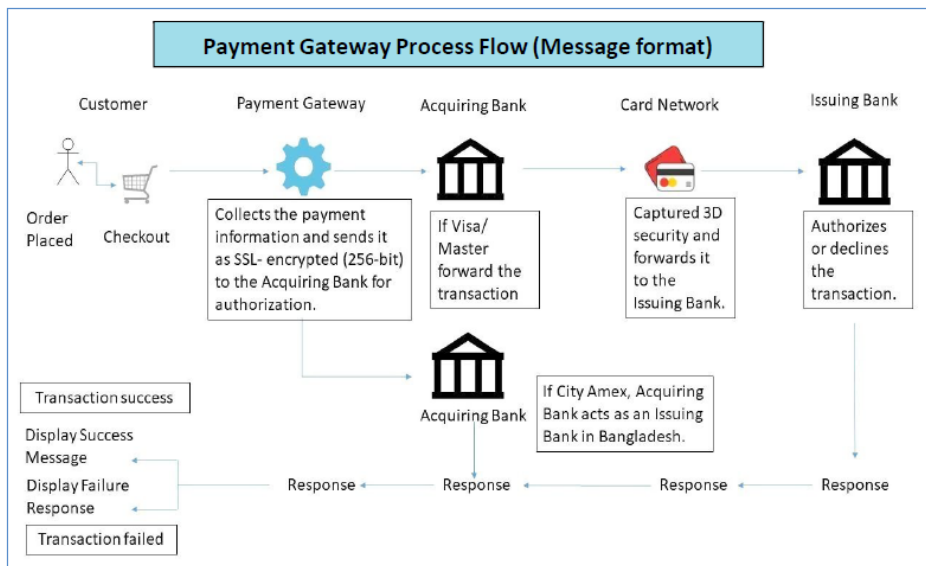


Diagram: Fund Flow

Integration with Banks, Merchants, Customers with PSO

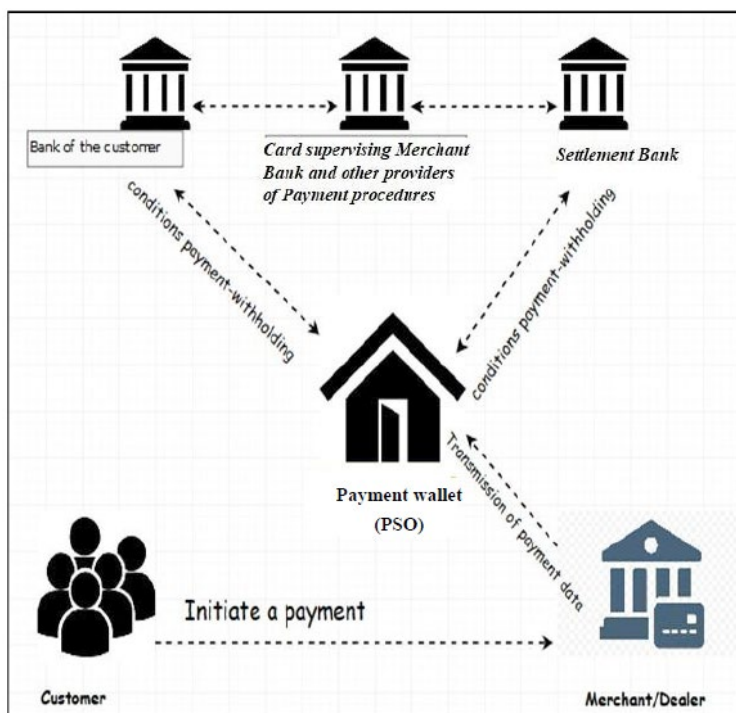







Diagram: Integration with Banks, Merchants, Customers with PSO

2.4 Others

We examine five elements or “pillars” which need to be addressed in order to ensure effective payments. These elements are critical to enabling fast and secure payment.

F i g u r e : F i v e k e	Security	Distribution	Devices (Front End)	Payment Processing (Back End)	Integration
	 Relates to the ability to confirm user identity for data and consumer protection.	 Geographical reach of financial services in terms of points of access. Also includes convenience of access.	 The range of front-end options available to citizens to access financial services.	 Refers to the back-end support systems and their capability to process payments.	 The extent to which Payment systems are interlinked.

Key pillars to facilitate driving effective digital transaction for PSO

3. Hardware Details

3.1 Value and Source

Value and sources of Different Hardware Are Software Components are explained below

Payment Gateways

A payment gateway is the software that sits among PSO’s site, End User interface and the financial institutes that processes the transactions. It functions by securely transmitting sensitive data, from an online payment form to a payment processor. It also allows you to not have to store that sensitive data on your website where it could be easily hacked.

In addition, it also provides behind the scenes, a payment gateway also supports things like recurring billing and virtual terminals in case users need to punch in the occasional phone order.

Payment Wallet has strong SDLC team who are capable to develop Payment gateway software in- house.

Payment Gateway Compatibility with Payment Processors

Some hybrid solutions exist where the payment gateway and the payment service provider are bundled together, such as with Stripe. We proposed customized solution that fits our needs.

Payment service operator hosting

To become an independent payment service operator, a business can either implement its own server infrastructure or use a third party hosting (such as amazon, fire hostor Rackspace). Local hosted server will be used by Payment Wallet for hosting.

Card Machines

Also known as a **payment terminal**, to-process card transactions. Card machines will use a connection via phone or internet to transmit the transaction details for present transactions that are swiped, keyed-in or dipped in the chip card reader.

We can also connect peripherals such as PIN pads and Near-Field Communication (NFC) readers for accepting “contact-less payments” such as Android or Apple Pay, although many newer machines have those built in.

Card Readers

These are the little card readers that will be connected with PC, smartphone or the tablet.

Virtual Terminals

Users can punch in the details of phone orders/mail orders via virtual terminal as long there is an internet connection. These either run as a standalone application on your computer or smartphone, or more often you just access a login URL in your web browser and process payments right in the browser window from any connected device.

Mobile Payment Processing

Payment Wallet is going to give users the ability to process mobile payments by default.

Flexible customization

Payment Wallet will setup and configure payment platform, to fit all your business-specific needs. Each user will get individual solution with free of charge setup.

Powerful fees and rates configuration

Our proposed software gives you maximum freedom in setting tariff plans for the users.

3.2 Module wise functionality

One of the greatest challenges for Payment Service Providers is the providing of high-quality software for the usage of their services. Due to our long lasting experience in this IT field, we know the daily challenges and can therefore offer an interesting solution.

Key Factor Payment Modules

Payment modules play a central part in PSO for several reasons.

- **Payment Module:** The payment modules are basically the business card of a Payment Service Provider. If the software doesn't work, the product cannot be sold. An increasingly negative image evolves and spreads among the communities. In the case of security gaps it may become especially uncomfortable. Considering all the facts Payment Wallet will develop payment modules software.

- **Support System Module:** The huge diversity of available shop systems makes it impossible for the Payment Service Provider and its support team to offer customer support for each shop system. Support module will be developed by Payment Wallet to overcome this problem.

- **Different Business Functional Modules under ERP:** From Accounting to Finance, Marketing to Advertisement, HR to Strategic, all functional modules will work under Centrally managed DB.

- In addition to that TPS, MIS, DSS and ESS modules will also be integrated under ERP.

Modules of e-Commerce where online payment gateway can be integrated to enable financial transaction:

- **B2C (Business-to-Consumer):** The business model where business sells products or service directly to consumers. B2C e-Commerce includes retail sales often called e-retail (or e-tail).

- **B2B (Business-to-Business):** The model whereby a company conducts its trading and other commercial activity through the net and the customer is the business itself. This essentially means commercial activity between companies through the internet as a medium.

- **C2C (Consumer-to-Consumer):** This is a business model that facilitates the transaction of products or services between customers. In these cases, a customer, not a business, sells goods or services to another customer.

- **B2G and G2B (Business to Govt. and Govt. to Business):** When a business sells its products or services to the government using computer network, it falls into B2G e-Commerce category and the vice versa is G2B.

- **M-Commerce (Mobile Commerce):** This is the commercial transactions that are conducted electronically by mobile phones. Known as next-generation e-Commerce, m-commerce enables users to access the Internet without needing to find a place to plug in.

Fraud Detection Module

We have implemented the below fraud detection module that covers following features:

1. Card issuer country - yes
2. Card issuer bank - yes
3. 3D Secure Value Authentication successful - yes or no (depending on acquiring bank)
4. 3D Secure Value Authentication attempted - yes or no (depending on acquiring bank)
5. 3D Secure Value Authentication not attempted - yes or no (depending on acquiring bank)
6. Daily Maximum Times of Transactions by a single card - 3
7. Weekly Maximum Times of Transactions by a single card - 21
8. Monthly Maximum Times of Transactions by a single card - 90
9. Cardholder IP- yes

Country of card issuance	3D Secure Value			Transaction Frequency		
	Authentication Successful (ECI: Visa 5, MC 2) yes or no	Authentication attempted (ECI: Visa 6, MC 1) yes or no	Authentication not attempted (ECI: Visa 7, MC 0) yes or no	Daily Maximum Times 3	Weekly Maximum Times 21	Monthly Maximum Times 90

The Solution: Payment Wallet/Payment Service Operator

Above mentioned modules are capable of handling the following

- Competence for over million online transactions.
- Will cover the entire integration field - from the Payment Page to a complete integration
- Personalized distribution platform will be created

3.3 PROPOSED DC AND DR SYSTEM:

Payment Wallet is IT centric, with information as the backbone of the business. Ensuring that information infrastructure that runs the business is disaster proof is extremely critical considering the cost implications of system down-times and information not available to the business.

Data Center Configuration and Details

Location: Square Informatix Ltd. Savar, Dhaka

SN	Description
01	Rack Space in Rack (600mm*1000mm) - Half Rack
02	POWER-AC Power with Generator back-up
03	Optical Fiber inside the exchange compound with ports and connectors in patch panel (ODF) at both ends
04	Bandwidth: 50 mbps
05	Media Converter (Including Power)-2 Media Converter need for both end

Server Configuration:

SN	Configuration Details
01	Intel® Skylake i7-6700 Quad-Core, up to 4x 4.0 GHz
02	RAM: DDR4 32 GB
03	HDD: 2x 2TB SATA II HDD, 7,2k
04	Connection: 1 Gbit/s
05	Backup: Acronis Backup Basic
06	Operating System: Linux (CentOS)
07	Platform: cPanel/WHM

Power Backup Plan: Provided by Square Informatix Ltd.

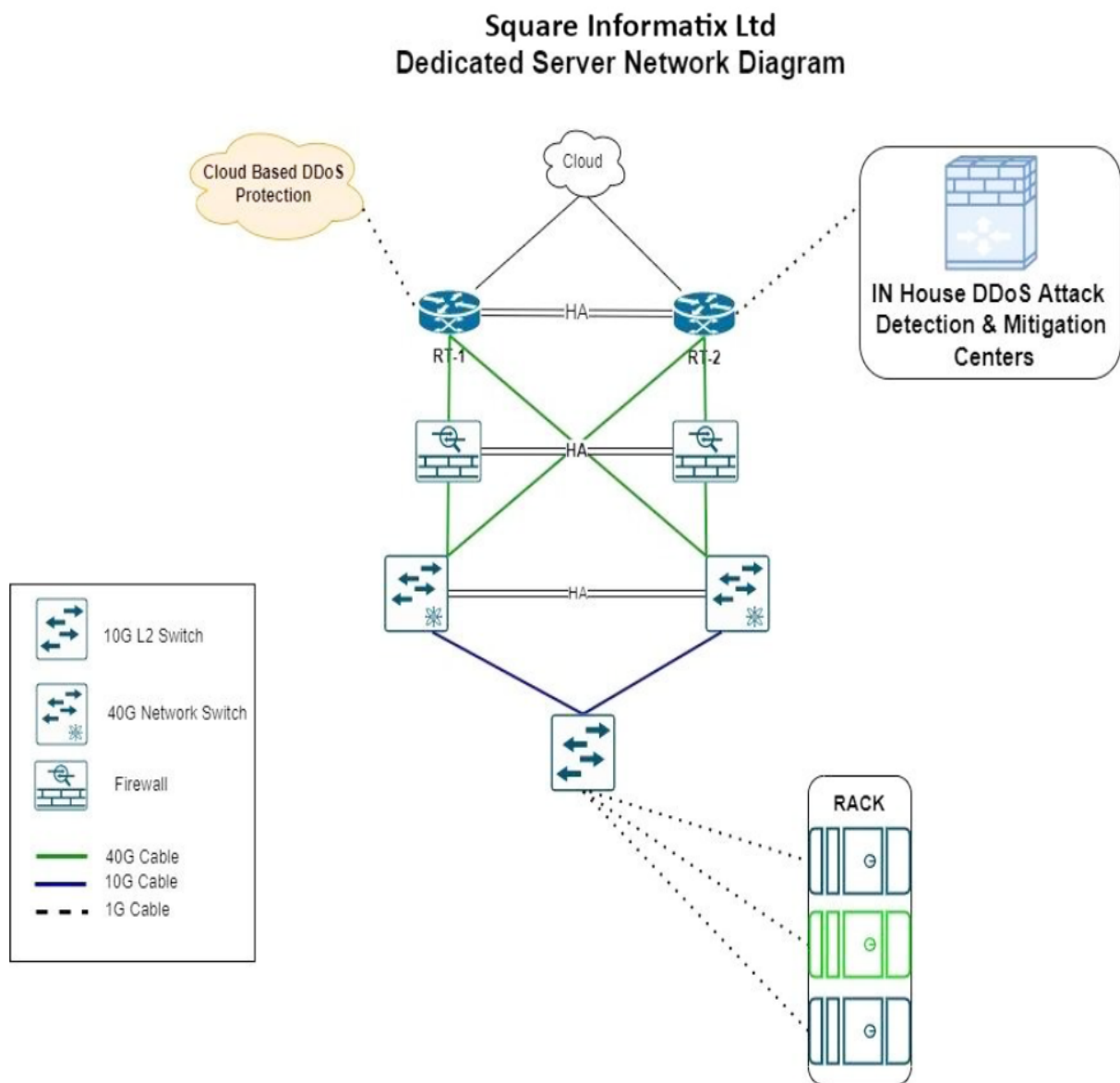
Software/Platform Details: cPanel/WHM with necessary plugins

DDoS Protection: Cloud-flare Protection

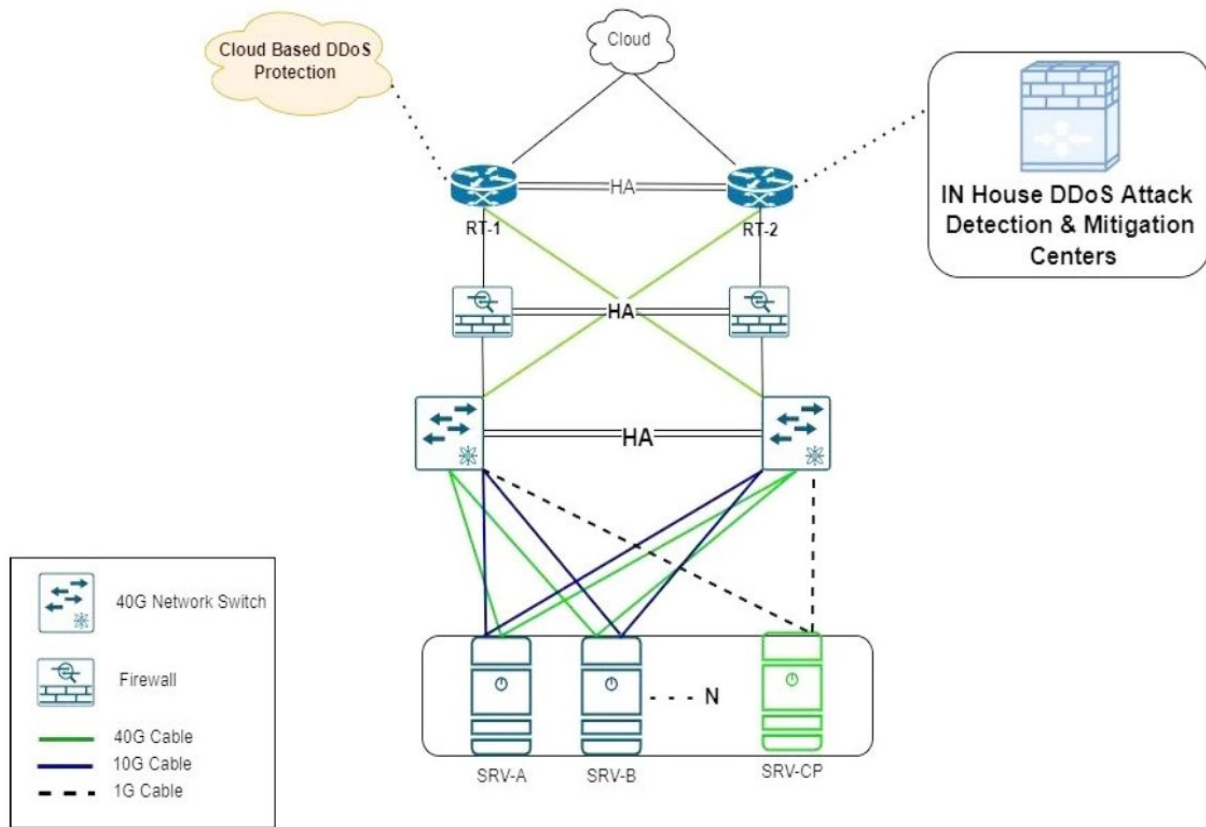
Load Balancer: Neutrino

Backup/Restore: CPREMOTE

- Can restore backup within 10 minutes,
- Recovery time depends on internet connection speed.



Square Informatix Ltd Cloud Network Diagram



Security and Firewall Details: ConfigServer Security & Firewall (csf)

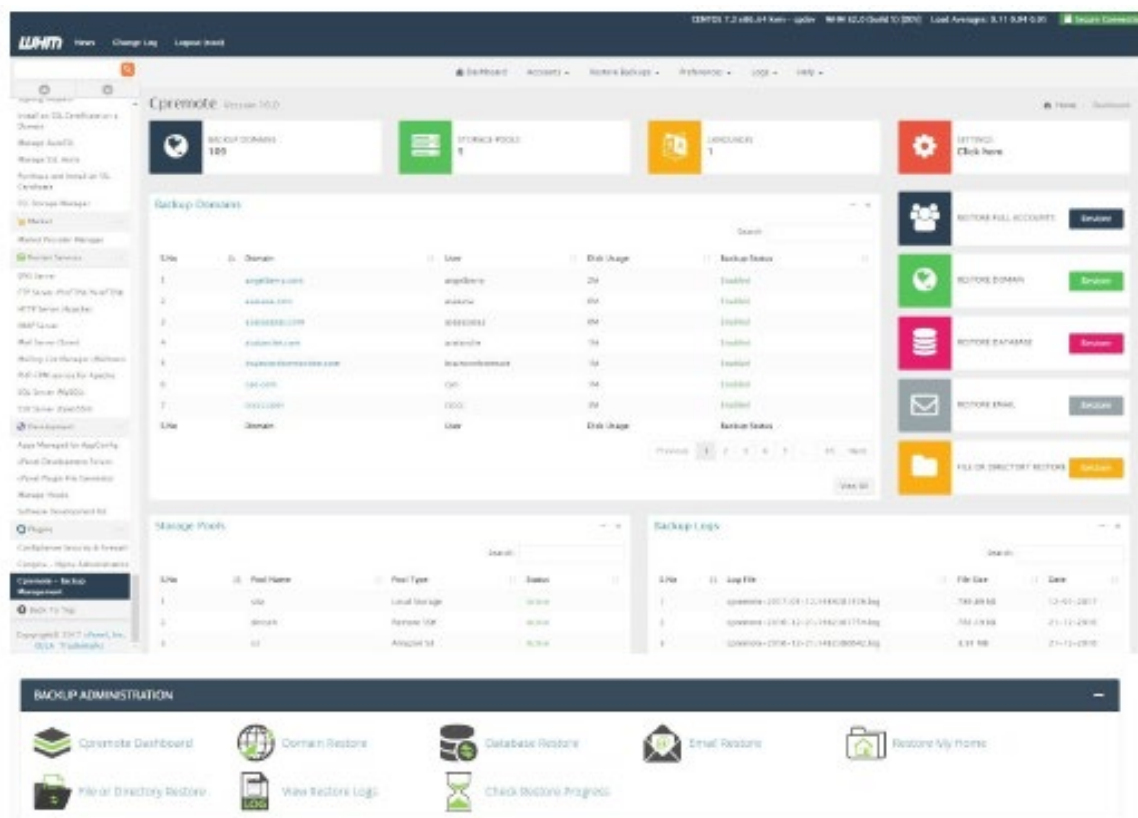
Features of Firewall:

- Straight-forward SPI iptables firewall script
- Daemon process that checks for login authentication failures for:
 - Courier imap, Dovecot, uw-imap, Kerio
- openSSH
- cPanel, WHM, Webmail (cPanel servers only)
- Pure-ftpd, vsftpd, Proftpd
- Password protected web pages (htpasswd)
- Mod_security failures (v1 and v2)
- Suhosin failures
- Exim SMTP AUTH
- Custom login failures with separate log file and regular expression matching
- POP3/IMAP login tracking to enforce logins per hour
- SSH login notification
- SU login notification
- Excessive connection blocking
- UI Integration for cPanel, DirectAdmin and Webmin

- Easy upgrade between versions from within cPanel/WHM, DirectAdmin or Webmin
- Easy upgrade between versions from shell
- Pre-configured to work on a cPanel server with all the standard cPanel ports open
- Pre-configured to work on a DirectAdmin server with all the standard DirectAdmin ports open
- Auto-configures the SSH port if it's non-standard on installation
- Block traffic on unused server IP addresses - helps reduce the risk to your server
- Alert when end-user scripts sending excessive emails per hour - for identifying spamming scripts
- Suspicious process reporting - reports potential exploits running on the server
- Excessive user processes reporting
- Excessive user process usage reporting and optional termination
- Suspicious file reporting - reports potential exploit files in /tmp and similar directories
- Directory and file watching - reports if a watched directory or a file changes
- Block traffic on a variety of Block Lists including DShield Block List and Spamhaus DROP List
- BOGON packet protection
- Pre-configured settings for Low, Medium or High firewall security (cPanel servers only)
- Works with multiple ethernet devices
- Server Security Check - Performs a basic security and settings check on the server (via cPanel/DirectAdmin/Webmin UI)
- Allow Dynamic DNS IP addresses - always allow your IP address even if it changes whenever you connect to the internet
- Alert sent if server load average remains high for a specified length of time
- mod_security log reporting (if installed)
- Email relay tracking - tracks all email sent through the server and issues alerts for excessive usage (cPanel servers only)
- IDS (Intrusion Detection System) - the last line of detection alerts you to changes to system and application binaries
- SYN Flood protection
- Ping of death protection
- Port Scan tracking and blocking
- Permanent and Temporary (with TTL) IP blocking
- Exploit checks
- Account modification tracking - sends alerts if an account entry is modified, e.g. if the password is changed or the login shell
- Shared syslog aware
- Messenger Service - Allows you to redirect connection requests from blocked IP addresses to preconfigured text and html pages to inform the visitor that they have been blocked in the firewall. This can be particularly useful for those with a large user base and help process support requests more efficiently

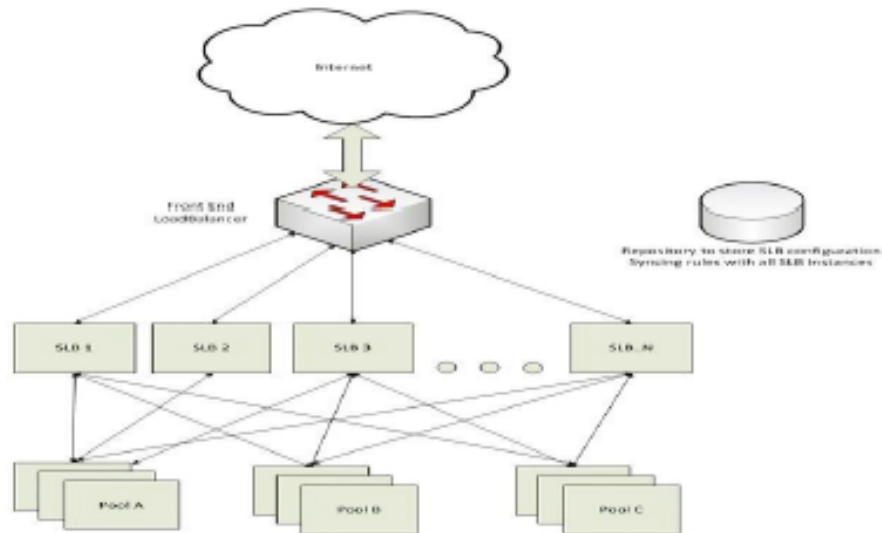
- Country Code blocking - Allows you to deny or allow access by ISO Country Code
- Port Flooding Detection - Per IP, per Port connection flooding detection and mitigation to help block DOS attacks
- DirectAdmin UI integration
- Updated Webmin UI integration
- WHM root access notification (cPanel servers only)
- Ifd Clustering - allows IP address blocks to be automatically propagated around a group of servers running Ifd. It allows allows cluster-wide allows, removals and configuration changes
- Quick start csf - deferred startup by Ifd for servers with large block and/or allow lists
- Distributed Login Failure Attack detection
- Temporary IP allows (with TTL)
- IPv6 Support with iptables
- Integrated UI - no need for a separate Control Panel or Apache to use the csf configuration
- Integrated support for cse within the Integrated UI
- cPanel Reseller access to per reseller configurable options Unblock, Deny, Allow and Search IP address blocks
- System Statistics - Basic graphs showing the performance of the server, e.g. Load Averages, CPU Usage, Memory Usage, etc
- ipset support for large IP lists
- Integrated with the CloudFlare Firewall

How CPREMOTE works:



Load Balancer Work Flow:

- Neutrino is used by eBay and built using Scala & Netty. It supports least-connection and round- robin algorithms with the following switching features.
- Using canonical names
- Context-based
- L4 using TCP port numbers



Data Recovery Center Configuration and Details

Location: Square Informatix Ltd. Savar, Dhaka

Server Configuration:

SN	Model	Description
01	Model	Dell PowerEdge R320 Server
02	Chassis Type	1-U Rack Mount
03	Processor	Intel Xeon E5-2407 v2 2.40GHz, 10M Cache, 6.4GT/s QPI, Turbo, 4C, 80W, Max Mem
04	No of processors	01 (One)
04	Chipset	Intel C600 Chipset
05	RAM	16GB Memory (2x8GB),RDIMM, 1600MT/s, Low Volt, Single Rank, x4 Data Width Up to 96GB (6 DIMM Slots)
06	Hard Drive	2 x 1TB 7.2K RPM NL-SAS, 6Gbps 3.5" Hot Plug Hard Drive
07	LAN /NIC	Integrated Dual Port 1GbE BASE-T
08	Remote Management	Baseboard Management Controller (12G)

Power Backup Plan: UPS (CyberPower) / Diesel Generator (Autostart)

Software/Platform Details: cPanel/WHM with necessary plugins

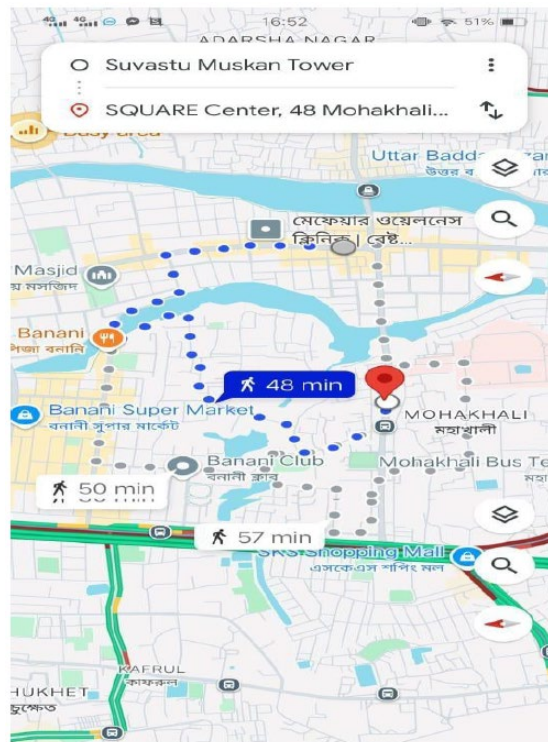
DDoS Protection: Cloudflare Protection Load Balancer: Neutrino

Backup/Restore: CPREMOTE

- Can restore backup within 10 minutes,
- Recovery time depends on internet connection speed

Connectivity: Two dedicated fiber optic based connection from two separate reputed ISP with dedicated Real IP

Distance: The distance between SIL (Data Center Server) and Payment Wallet Office (Data Recovery Server) is showing more than 10 KM as shared by google maps screenshot below.



Security and Firewall Details: ConfigServer Security & Firewall (csf)

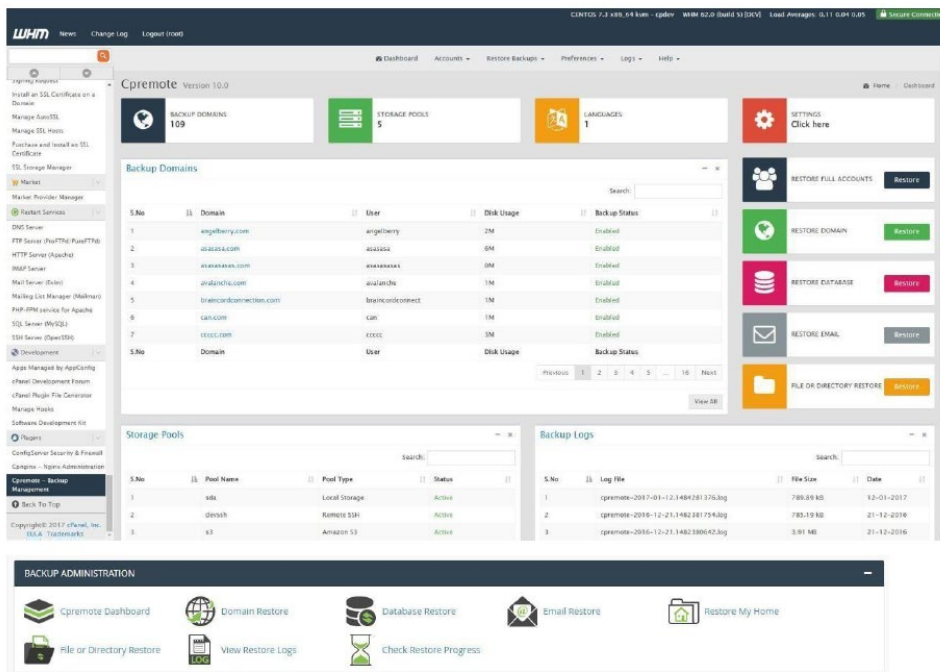
Features of Firewall:

- Straight-forward SPI iptables firewall script
- Daemon process that checks for login authentication failures for:
 - Courier imap, Dovecot, uw-imap, Kerio
 - openSSH
 - cPanel, WHM, Webmail (cPanel servers only)
 - Pure-ftpd, vsftpd, Proftpd
 - Password protected web pages (htpasswd)
 - Mod_security failures (v1 and v2)
 - Suhosin failures
 - Exim SMTP AUTH

- Custom login failures with separate log file and regular expression matching
- POP3/IMAP login tracking to enforce logins per hour
- SSH login notification
- SU login notification
- Excessive connection blocking
- UI Integration for cPanel, DirectAdmin and Webmin
- Easy upgrade between versions from within cPanel/WHM, DirectAdmin or Webmin
- Easy upgrade between versions from shell
- Pre-configured to work on a cPanel server with all the standard cPanel ports open
- Pre-configured to work on a DirectAdmin server with all the standard DirectAdmin ports open
- Auto-configures the SSH port if it's non-standard on installation
- Block traffic on unused server IP addresses - helps reduce the risk to your server
- Alert when end-user scripts sending excessive emails per hour - for identifying spamming scripts
- Suspicious process reporting - reports potential exploits running on the server
- Excessive user processes reporting
- Excessive user process usage reporting and optional termination
- Suspicious file reporting - reports potential exploit files in /tmp and similar directories
- Directory and file watching - reports if a watched directory or a file changes
- Block traffic on a variety of Block Lists including DShield Block List and Spamhaus DROP List
- BOGON packet protection
- Pre-configured settings for Low, Medium or High firewall security (cPanel servers only)
- Works with multiple ethernet devices
- Server Security Check - Performs a basic security and settings check on the server (via cPanel/DirectAdmin/Webmin UI)
- Allow Dynamic DNS IP addresses - always allow your IP address even if it changes whenever you connect to the internet
- Alert sent if server load average remains high for a specified length of time
- mod_security log reporting (if installed)
- Email relay tracking - tracks all email sent through the server and issues alerts for excessive usage (cPanel servers only)
- IDS (Intrusion Detection System) - the last line of detection alerts you to changes to system and application binaries
- SYN Flood protection

- Ping of death protection
- Port Scan tracking and blocking
- Permanent and Temporary (with TTL) IP blocking
- Exploit checks
- Account modification tracking - sends alerts if an account entry is modified, e.g. if the password is changed or the login shell
- Shared syslog aware
- Messenger Service - Allows you to redirect connection requests from blocked IP addresses to preconfigured text and html pages to inform the visitor that they have been blocked in the firewall. This can be particularly useful for those with a large user base and help process support requests more efficiently
- Country Code blocking - Allows you to deny or allow access by ISO Country Code
- Port Flooding Detection - Per IP, per Port connection flooding detection and mitigation to help block DOS attacks
- DirectAdmin UI integration
- Updated Webmin UI integration
- WHM root access notification (cPanel servers only)
- lfd Clustering - allows IP address blocks to be automatically propagated around a group of servers running lfd. It allows cluster-wide allows, removals and configuration changes
- Quick start csf - deferred startup by lfd for servers with large block and/or allow lists
- Distributed Login Failure Attack detection
- Temporary IP allows (with TTL)
- IPv6 Support with ip6tables
- Integrated UI - no need for a separate Control Panel or Apache to use the csf configuration
- Integrated support for cse within the Integrated UI
- cPanel Reseller access to per reseller configurable options Unblock, Deny, Allow and Search IP address blocks
- System Statistics - Basic graphs showing the performance of the server, e.g. Load Averages, CPU Usage, Memory Usage, etc
- ipset support for large IP lists
- Integrated with the Cloud-flare Firewall

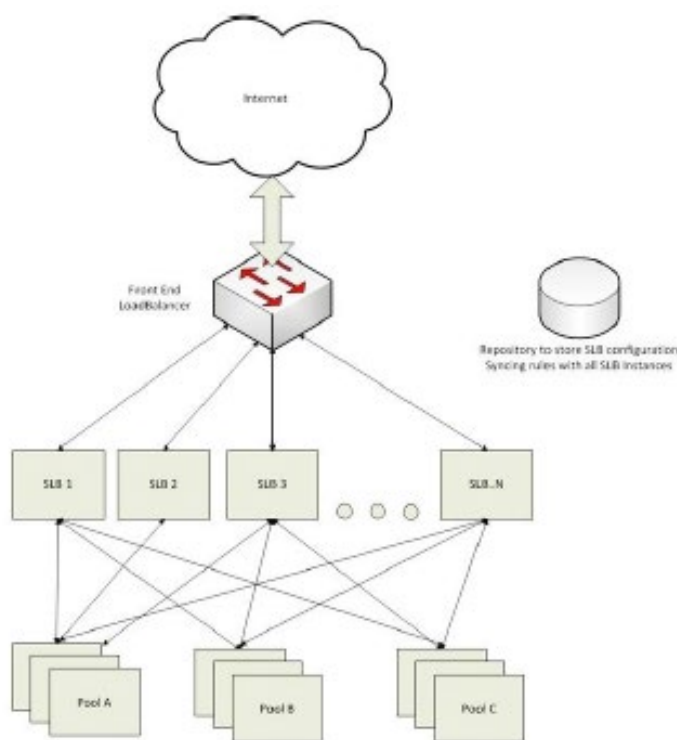
How CPREMOTE works:



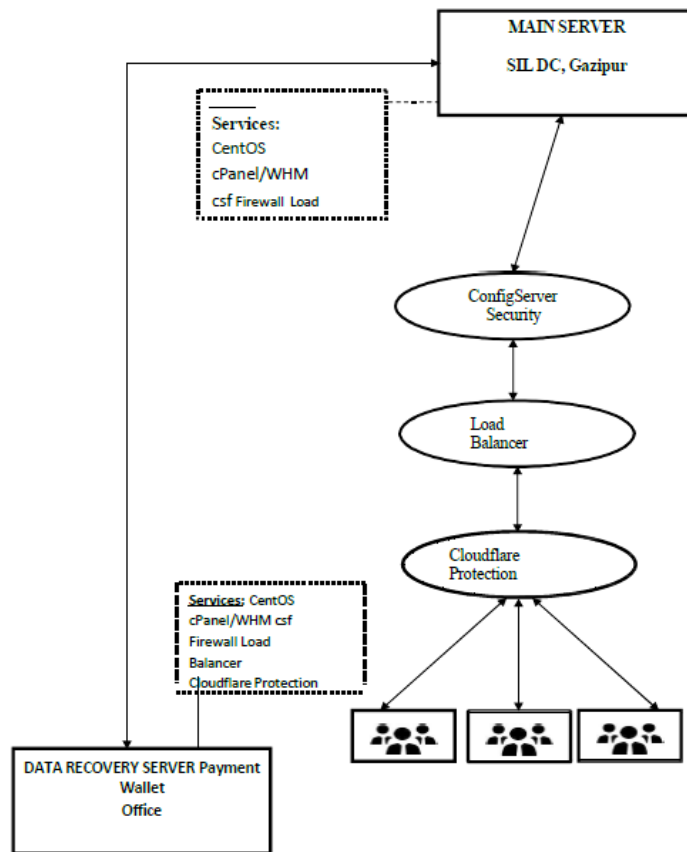
Load Balancer Work Flow:

Neutrino is used by eBay and built using Scala & Netty. It supports least-connection and round-robin algorithms with the following switching features.

- Using canonical names
- Context-based
- L4 using TCP port numbers



Plan Diagram



3.4 USER CAPACITY, TPS AND SESSION

High-load ready

Through our software Payment Wallet can process more than 300 transactions per second (TPS) without using expensive enterprise software or hardware. We route the transactions based on our algorithm set in our payment gateway software. When there is large number of transactions the algorithm automatically redirects to a free bank payment gateway to reduce heavy load.

Anti-fraud instruments

Our solution uses integrated checks and rules configuration for each payment transaction. Also can use popular scoring systems to ensure minimum fraud transactions level.

Fraud Detection Module

We have implemented the below fraud detection module that covers following features:

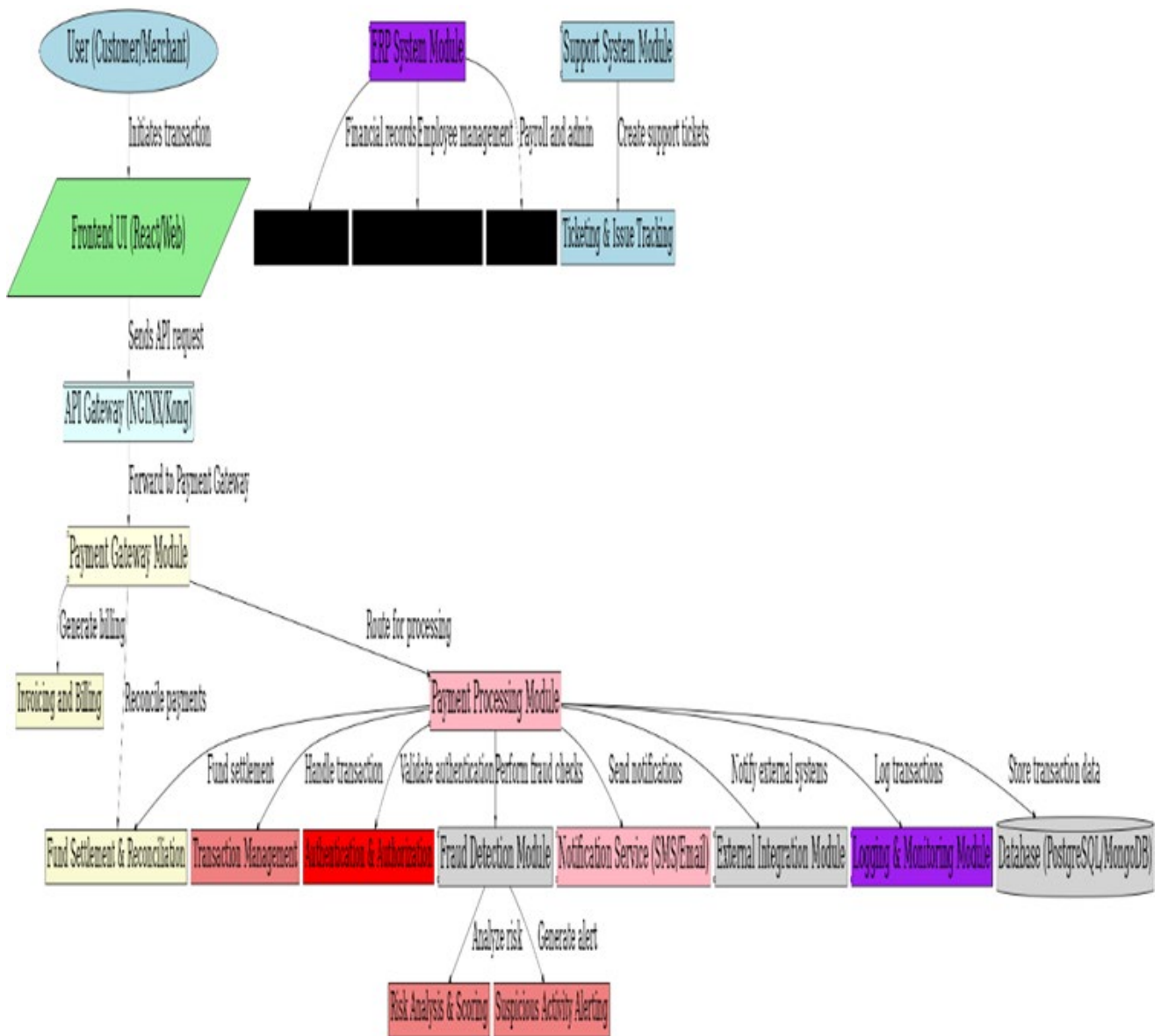
1. Card issuer country - Yes
2. Card issuer bank - Yes
3. 3D Secure Value Authentication successful - yes or no (depending on acquiring bank)
4. 3D Secure Value Authentication attempted - yes or no (depending on acquiring bank)
5. 3D Secure Value Authentication not attempted - yes or no (depending on acquiring bank)
6. Daily Maximum Times of Transactions by a single card - 3
7. Weekly Maximum Times of Transactions by a single card - 21
8. Monthly Maximum Times of Transactions by a single card - 90
9. Cardholder IP- Yes

Country of card issuance	3D Secure Value			Transaction Frequency		
	Authentication Successful (ECI: Visa 5, MC 2) yes or no	Authentication attempted (ECI: Visa 6, MC 1) yes or no	Authentication not attempted (ECI: Visa 7, MC 0) yes or no	Daily Maximum Times 3	Weekly Maximum Times 21	Monthly Maximum Times 90

Fault tolerance

We can provide different fault tolerance schemes, that depends upon our infrastructure.

4. Software details



4.1 Value and Source

Value and sources of Different Hardware Are Software Components are explained below

Billing and Invoicing

Our platform gave you full cycle solution to support all areas of Payment Service Provider business. Software will automate invoicing and billing to control all settlements with your clients. Billing and Invoicing software will be developed by in house team of Payment Wallet and hardware will be procured from renewed company

Secure payment card data storage

Our software will be licensed according to strict security standards. It will allow Bangladesh Bank and Regulatory Authority to easily pass PCI DSS audit and you can be sure, that customer's card data stored with maximum safety. Compliance and card storage system will be developed by in house team of Payment Wallet and hardware will be procured from reputed company providing highest security.

ERP systems

To fully automate our company Payment Wallet will go for modular solution. All modules (Finance & Accounts, HR, Admin, Payroll, Marketing) will be managed and controlled by centrally managed Data Base. We will use Oracle for Back end, Java and Php for Front End.

4.2 Module wise functionality

One of the greatest challenges for Payment Service Providers is the providing of high-quality software for the usage of their services. Due to our long lasting experience in this IT field, we know the daily challenges and can therefore offer an interesting solution.

Key Factor Payment Modules

Payment modules play a central part in PSO for several reasons.

- **Payment Module:** The payment modules are basically the business card of a Payment Service Provider. If the software doesn't work, the product cannot be sold. An increasingly negative image evolves and spreads among the communities. In the case of security gaps it may become especially uncomfortable. Considering all the facts Payment Wallet will develop payment modules software.
- **Support System Module:** The huge diversity of available shop systems makes it impossible for the Payment Service Provider and its support team to offer customer support for each shop system. Support module will be developed by Payment Wallet to overcome this problem.
- **Different Business Functional Modules under ERP:** From Accounting to Finance, Marketing to Advertisement, HR to Strategic, all functional modules will work under Centrally managed DB
- In addition to that TPS, MIS, DSS and ESS modules will also be integrated under ERP.

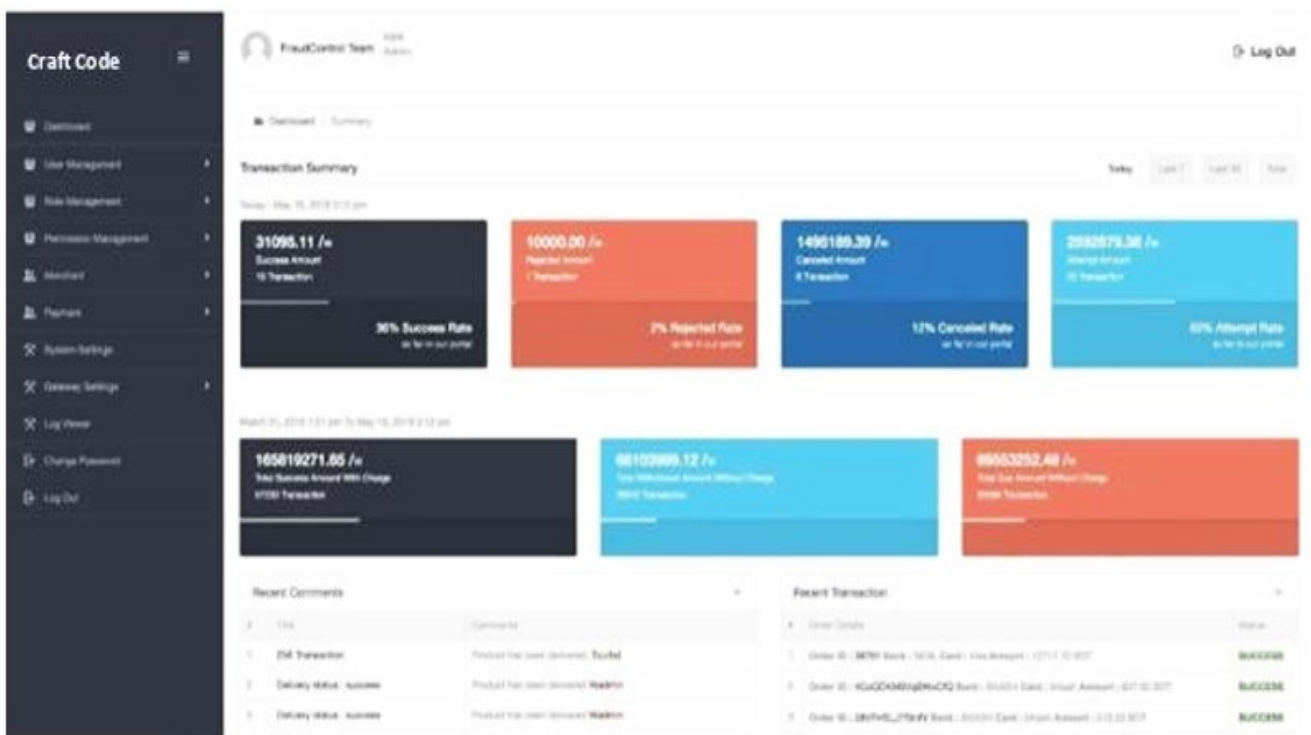
Fraud Detection Module

We have implemented the below fraud detection module that covers following features:

1. Card issuer country - Yes
2. Card issuer bank - Yes
3. 3D Secure Value Authentication successful - yes or no (depending on acquiring bank)
4. 3D Secure Value Authentication attempted - yes or no (depending on acquiring bank)
5. 3D Secure Value Authentication not attempted - yes or no (depending on acquiring bank)
6. Daily Maximum Times of Transactions by a single card - 3
7. Weekly Maximum Times of Transactions by a single card - 21
8. Monthly Maximum Times of Transactions by a single card - 90
9. Cardholder IP- Yes

Country of card issuance	3D Secure Value			Transaction Frequency		
	Authentication Successful (ECI: Visa 5, MC 2) yes or no	Authentication attempted (ECI: Visa 6, MC 1) yes or no	Authentication not attempted (ECI: Visa 7, MC 0) yes or no	Daily Maximum Times	Weekly Maximum Times	Monthly Maximum Times
				3	21	90

4.3 Payment Gateway Software



Dashboard View

ProductCentral Team 1000 Users Log Out

Dashboard > Transaction

Transaction Filter

Merchant ID	Merchant ID	Username	Username	Website	Website
Date Range	Date Range	Merchant Order ID	Merchant Order ID	Merchant Order ID	Merchant Order ID
Min Amount	Min Amount	Max Amount	Min Amount	Card Number	Card Number
Bank	Select Bank	Payment Method	Payment Method	Transaction Status	No Filter
Transaction	Select One	Bank Status	No Status	Transaction ID	Transaction ID
Customer Details	Name Email Phone Address	Payment Completion	Select One	Reference ID	Reference ID
Merchant Name ID	Merchant Name ID	Other Details	Other Details	Transaction Type	Select Transaction

Search Number:

1 2 3 4 5 6 7 8 ... 292 293

Search Number:

1 2 3 4 5 6 7 8 ... 160 161

SL	Merchant Order Details	Merchant Transaction Details	Card & Customer Details	Other Details	View
1	<p>Website Trn ID: 16018</p> <p>Merchant Order ID: 16018</p> <p>City Bank ID: 819163880</p> <p>Bank: CDB</p> <p>Reference ID: 81916388025478</p> <p>Merchant ID: 81916388025478</p> <p>Foreign Transaction</p> <p>Website: Nanyang.com</p> <p>Process Completion: 100%</p>	<p>Merchant Amount: 1283.00 BDT</p> <p>Card Charge: 44.23 BDT on 2.83 %</p> <p>Extra Charge: Merchant (1)</p> <p>Paid Amount: 1327.23 BDT</p> <p>MSB Payout Amount: 1219.17 BDT</p> <p>Request ID: 175.32.202.14</p> <p>Bank Status: SUCCESS</p> <p>MSB Status: REQUEST FOR VERIFICATION</p> <p>Review Status: NOT PAID</p>	<p>Card Number: 401200000111</p> <p>Brand: VISA</p> <p>Card Holder: SAAD KHAN</p> <p>Country: Canada</p> <p>Card Type: credit</p> <p>MSB Payout Amount: 119.80 BDT</p> <p>MSB Payout Ref: 81916388025478</p> <p>Merchant Name: Nanyang.com</p> <p>Request Time: 12 May 2018 10:20 pm</p> <p>Exp Time: 12 May 2018 10:30 pm</p>	<p>Product Details</p> <p>TUMIX Turn Up Laptop 13.3" - 75.311</p> <p>Product Weight (gms) 214976</p> <p>Estimated Expansive Weight 7000000</p> <p>SKU 14981 Turn Note Open-M4</p> <p>Returning Expansive Fee 52716-0102</p> <p>Shipping Weight (kg) 2.83</p> <p>amount 142.42-1283.00</p>	<p><input type="button" value="Details"/> <input type="button" value="Invoice"/></p> <p><input type="button" value="Link"/></p> <p><input type="button" value="Comment"/></p> <p><input type="button" value="Review"/></p> <p>Request for Verification</p>
2	<p>Website Trn ID: 16043</p> <p>Merchant Order ID: 16043</p> <p>City Bank ID: 819163880</p> <p>Bank: CDB</p> <p>Card: Master</p> <p>Reference ID: 81916388025478</p> <p>Merchant ID: 81916388025478</p> <p>Foreign Transaction</p> <p>Website: charls.expansive.com</p> <p>Process Completion: 100%</p>	<p>Merchant Amount: 15.99 USD</p> <p>Merchant Amount: 1599.15 BDT</p> <p>Card Charge: 42.48 BDT on 2.63 %</p> <p>Extra Charge: Merchant (1)</p> <p>Paid Amount: 1641.63 BDT</p> <p>MSB Payout Amount: 1586.67 BDT</p> <p>Request ID: 144.48.152.24</p> <p>Bank Status: SUCCESS</p> <p>MSB Status: REQUEST FOR VERIFICATION</p> <p>Review Status: NOT PAID</p>	<p>Card Number: 5400000000000</p> <p>Brand: MFC</p> <p>Card Holder: 884 Nafay Khan</p> <p>Country: Canada</p> <p>Card Type: credit</p> <p>MSB Payout Ref: 1599.15 BDT</p> <p>merchantid@gmail.com, Dr. Dr. Dr. Dr.</p> <p>Phone: 7278</p> <p>Request Time: 12 May 2018 12:30 pm</p> <p>Exp Time: 12 May 2018 12:40 pm</p>	<p>Product Details</p> <p>Expansive - Invoice #16043</p>	<p><input type="button" value="Details"/> <input type="button" value="Invoice"/></p> <p><input type="button" value="Link"/></p> <p><input type="button" value="Comment"/></p> <p><input type="button" value="Review"/></p> <p>Request for Verification</p>

SL	Merchant Order Details	Merchant Transaction Details	Card & Customer Details	Other Details	View
1	<p>Website Trn ID: 16096</p> <p>Merchant Order ID: 1708</p> <p>City Bank ID: 8000000000000</p> <p>Bank: DBBL</p> <p>Card: Visa</p> <p>Reference ID: 8000000000000</p> <p>Merchant ID: 8000000000000</p> <p>Local Transaction</p> <p>Website: alharraq.com</p> <p>Process Completion: 100%</p>	<p>Merchant Amount: 8296.00 BDT</p> <p>Card Charge: 198.42 BDT on 2.39 %</p> <p>Extra Charge: Card Holder (1)</p> <p>Paid Amount: 8494.42 BDT</p> <p>MSB Payout Amount: 8296.00 BDT</p> <p>Request ID: 182.163.132.234</p> <p>Bank Status: SUCCESS</p> <p>MSB Status: NOT PAID</p>	<p>Card Number: 4442000000000</p> <p>Brand: Card</p> <p>Country: Bangladesh</p> <p>Card Type: credit</p> <p>Merchant Name: 1708000000</p> <p>merchantid@gmail.com, Dr. Dr. Dr. Dr.</p> <p>Merchant Website: alharraq.com</p> <p>Phone: 1212</p> <p>Request Time: 29 May 2018 12:48 pm</p> <p>Exp Time: 29 May 2018 12:58 pm</p>	<p>Product Details</p> <p>Alharraq - Invoice #1708</p>	<p><input type="button" value="Details"/> <input type="button" value="Invoice"/></p> <p><input type="button" value="Link"/></p> <p><input type="button" value="Comment"/></p> <p><input type="button" value="Review"/></p> <p>Success</p>
2	<p>Website Trn ID: 16107</p> <p>Merchant Order ID: 1704</p> <p>City Bank ID: 8000000000000</p> <p>Bank: DBBL</p> <p>Card: Visa</p> <p>Reference ID: 8000000000000</p> <p>Merchant ID: 8000000000000</p> <p>Local Transaction</p> <p>Website: yashkari.com</p> <p>Process Completion: 100%</p>	<p>Merchant Amount: 206.00 BDT</p> <p>Card Charge: 12.42 BDT on 2.63 %</p> <p>Extra Charge: Merchant (1)</p> <p>Paid Amount: 218.42 BDT</p> <p>MSB Payout Amount: 206.00 BDT</p> <p>Request ID: 182.163.132.234</p> <p>Bank Status: SUCCESS</p> <p>MSB Status: PAID</p>	<p>Card Number: 4442000000000</p> <p>Brand: National</p> <p>Country: Bangladesh</p> <p>Card Type: credit</p> <p>Merchant Name: 1704000000</p> <p>merchantid@gmail.com, Pak. No. 20,</p> <p>House No. 198, Road No. 26, Saha Union</p> <p>Hojaj Bazar, Dhaka, Dhaka 1212,</p> <p>Phone: 1212</p> <p>Request Time: 27 May 2018 8:15 pm</p> <p>Exp Time: 27 May 2018 8:25 pm</p>	<p>Cardholder.com Details</p> <p>Payment Type: Verification Payment</p> <p>Product Details</p> <p>Powerful 300-3000mAh battery 16119</p> <p>amount amount 0-206.00</p>	<p><input type="button" value="Details"/> <input type="button" value="Invoice"/></p> <p><input type="button" value="Link"/></p> <p><input type="button" value="Comment"/></p> <p><input type="button" value="Review"/></p> <p>Fail</p>
3	<p>Website Trn ID: 16086</p> <p>Merchant Order ID: 2717</p> <p>City Bank ID: 8000000000000</p> <p>Bank: DBBL</p> <p>Card: Visa</p> <p>Reference ID: 8000000000000</p> <p>Merchant ID: 8000000000000</p> <p>Local Transaction</p> <p>Website: shafiqulhasan.com</p> <p>Process Completion: 100%</p>	<p>Merchant Amount: 166.00 BDT</p> <p>Card Charge: 2.30 BDT on 2.05 %</p> <p>Extra Charge: Card Holder (1)</p> <p>Paid Amount: 168.30 BDT</p> <p>MSB Payout Amount: 166.00 BDT</p> <p>Request ID: 182.163.132.234</p> <p>Bank Status: SUCCESS</p> <p>MSB Status: NOT PAID</p>	<p>Card Number: 4442000000000</p> <p>Brand: National</p> <p>Country: Bangladesh</p> <p>Card Type: credit</p> <p>Merchant Name: 2717000000</p> <p>merchantid@gmail.com,</p> <p>Merchant: shafiqulhasan.com</p> <p>Phone: 1212</p> <p>Request Time: 30 Apr 2018 1:34 pm</p> <p>Exp Time: 30 Apr 2018 1:44 pm</p>	<p>Product Details</p> <p>PLUJ Hood - Invoice #1717</p>	<p><input type="button" value="Details"/> <input type="button" value="Invoice"/></p> <p><input type="button" value="Link"/></p> <p><input type="button" value="Comment"/></p> <p><input type="button" value="Review"/></p>

Payment Wallet Online Payment Gateway Software Features

Accepted Instruments

Payment Wallet accepts, verifies, and processes a variety of transaction instruments on behalf of the online businesses. The various instruments include:

- Credit cards
- Debit cards
- Bank Accounts
- Internet Banking Mobile Banking Payment Wallet connects online store shopping cart with a number of payment options at payment processor and/or bank end via a secure payment pages, forms, or payment APIs. Payment Wallet also have the ability to respond back with the payment status to the online store over appropriate and secured interfaces.

Features

Payment Wallet is enabling the online businesses in Bangladesh and abroad to accept payments in a secured manner. Payment Wallet incorporates the most stringent security levels along with checks and balances in every place and stage ensuring a total end-to-end protection of client's personal and sensitive information.

The following are some of the features available in the system:

- Supports all major domestic and International credit cards & domestic bank transfers (over secured connectivity to the payment processor).
- Uses industry standard SSL (Secure Sockets Layer) technology enabling 256-Bit SSL Encryption when exchanging sensitive client information.
- Multiple and easy payment methods
- Merchant login system
- Wide ranges of transaction reporting for merchants
- High level security management
- Fraud detection including invalid purchases
- Payment failure notification & Advantage of canceling payment
- Cross checking of a payment for a purchase from the online store
- Payment handling in Bangladeshi Taka (BDT)
- Provides support to online businesses in setting up merchant accounts.

Benefits

Payment Wallet makes it easy for online businesses, online retailers, bricks and clicks, or traditional brick and mortar merchants to accept payments anytime - anywhere. You can process credit cards, debit bank cards, bank accounts 24/7/365 because it never closes. The gateway setup is almost effortless, payment transactions are processed in real-time, and you have immediate control of your payment gateway and credit card payment data. Payment Wallet provides the most powerful payment system on the market and follows the security requirements set forth by Visa and MasterCard, as well as other secured ISO protocol technology.

It brings the following benefits for the online stores:

- Easy installation, operation & management
- Single Platform for all payments (Credit Card, Debit Card, Bank Account, etc.)
- Real-Time Transactions and real time transactional web reporting
- Centralized & secure data management
- Enables merchant to conduct business with ANYONE, ANYWHERE, ANYTIME!
- Settlement of funds on a regular basis

The Solution: Payment Wallet Payment Service Operator

Above mentioned modules are capable of handling the following

- Competence for over million online transactions.
- Will cover the entire integration field - from the Payment Page to a complete integration
- Personalized distribution platform will be created

4.4 PROPOSED DC AND DR SYSTEM:

Carft Code Ltd. proposed rebranded payment gateway service "Payment Wallet" is IT centric, with information as the backbone of the business. Ensuring that information infrastructure that runs the business is disaster proof is extremely critical considering the cost implications of system downtimes and information not available to the business.

Data Center Configuration and Details

Data Center Site Name: SIL DC

Location: Square Informatix Ltd. Gazipur, Dhaka

Data Center Site Facility:

1. Data Center Standard Tier-III (Concurrently Maintainable)
2. Data Center Space Data Center Space 8,000 sqf (total)
3. Generator & UPS System Redundant N+N Generators N+N UPS
4. Power Dual 16A commando socket Dual 32A commando socket
5. Precision Cooling TWO Sets N+1 Precision AC
6. Rack measurement 42U Containment Rack 600mm (W) x 1000mm (D) x 1869mm (H)
7. Safety Security Environment Monitoring & Control System. VESDA System Fire Detectors
Water Leak Defectors FM 200 Suppression System Physical Security
8. Designated to achieve 99.98% Uptime
9. Facilities Management 24x365 NOC

Data Center Server Configuration:

Processor	Core 4
Memory	RAM 8 GB
Hard Disk Drive	HDD 100GB
Connectivity	Internet 10 Mbps, BDIX 20 Mbps
Operating System	Cloud Linux
Software Platform	cPanel with necessary plug-ins
Power Backup Plan:	Provided by Square Informatix Ltd.

Security and Firewall Details: ConfigServer Security & Firewall (csf)

Features of Firewall:

- Straight-forward SPI iptables firewall script
- Daemon process that checks for login authentication failures for:
 - Courier imap, Dovecot, uw-imap, Kerio
 - openSSH
 - cPanel, WHM, Webmail (cPanel servers only)
 - Pure-ftpd, vsftpd, Proftpd
 - Password protected web pages (htpasswd)
 - Mod_security failures (v1 and v2)
 - Suhosin failures
 - Exim SMTP AUTH
- Custom login failures with separate log file and regular expression matching
- POP3/IMAP login tracking to enforce logins per hour
- SSH login notification

- SU login notification
- Excessive connection blocking
- UI Integration for cPanel, DirectAdmin and Webmin
- Easy upgrade between versions from within cPanel/WHM, DirectAdmin or Webmin
- Easy upgrade between versions from shell
- Pre-configured to work on a cPanel server with all the standard cPanel ports open
- Pre-configured to work on a DirectAdmin server with all the standard DirectAdmin ports open
- Auto-configures the SSH port if it's non-standard on installation
- Block traffic on unused server IP addresses - helps reduce the risk to your server
- Alert when end-user scripts sending excessive emails per hour - for identifying spamming scripts
- Suspicious process reporting - reports potential exploits running on the server
- Excessive user processes reporting
- Excessive user process usage reporting and optional termination
- Suspicious file reporting - reports potential exploit files in /tmp and similar directories
- Directory and file watching - reports if a watched directory or a file changes
- Block traffic on a variety of Block Lists including DShield Block List and Spamhaus DROP List
- BOGON packet protection
- Pre-configured settings for Low, Medium or High firewall security (cPanel servers only)
- Works with multiple ethernet devices
- Server Security Check - Performs a basic security and settings check on the server (via cPanel/DirectAdmin/Webmin UI)
- Allow Dynamic DNS IP addresses - always allow your IP address even if it changes whenever you connect to the internet
- Alert sent if server load average remains high for a specified length of time
- mod_security log reporting (if installed)
- Email relay tracking - tracks all email sent through the server and issues alerts for excessive usage (cPanel servers only)
- IDS (Intrusion Detection System) - the last line of detection alerts you to changes to system and application binaries
- SYN Flood protection
- Ping of death protection
- Port Scan tracking and blocking
- Permanent and Temporary (with TTL) IP blocking
- Exploit checks

- Exploit checks
- Account modification tracking - sends alerts if an account entry is modified, e.g. if the password is changed or the login shell
- Shared syslog aware
- Messenger Service - Allows you to redirect connection requests from blocked IP addresses to preconfigured text and html pages to inform the visitor that they have been blocked in the firewall.
- This can be particularly useful for those with a large user base and help process support requests more efficiently
- Country Code blocking - Allows you to deny or allow access by ISO Country Code
- Port Flooding Detection - Per IP, per Port connection flooding detection and mitigation to help block DOS attacks
- DirectAdmin UI integration
- Updated Webmin UI integration
- WHM root access notification (cPanel servers only)
- lfd Clustering - allows IP address blocks to be automatically propagated around a group of servers running lfd. It allows cluster-wide allows, removals and configuration changes
- Quick start csf - deferred startup by lfd for servers with large block and/or allow lists
- Distributed Login Failure Attack detection
- Temporary IP allows (with TTL)
- IPv6 Support with iptables
- Integrated UI - no need for a separate Control Panel or Apache to use the csf configuration
- Integrated support for cse within the Integrated UI
- cPanel Reseller access to per reseller configurable options Unblock, Deny, Allow and Search IP address blocks
- System Statistics - Basic graphs showing the performance of the server, e.g. Load Averages, CPU Usage, Memory Usage, etc
- ipset support for large IP lists
- Integrated with the CloudFlare Firewall

Data Recovery Center Configuration and Details

Data Recovery Site Name: Square Informatix Ltd.

Location: Square Centre (11th Floor), 48, Mohakhali C/A, Dhaka-1212, Bangladesh.

Data Recovery Site facility:

- 10,000 SQF stat of the art data center facility.
- 180 COLD AISLE CONTAINMENT RACKs capacity.
- N+N redundant UPS in every datacenter for uptime
- Automated Multiple Redundant diesel generators
- Dual power PDU in each rack
- Power racks ranging from 4KW to10KW
- Datacenter suite available for collocation services
- Metered PDU for rack level power monitoring and billing
- Redundant Air-Conditioned DC Environment
- N+1 precision air conditioner to maintain 20+/-1°C temperature and 50+/-5% relative humidity
- Cold aisle containments are implemented in two rows, containments are fabricated in stronger aluminum frames & Acrylic sheets
- Use of vermiculite material for green solution datacenter
- Fire-Protected Facility
- The highly advance laser based very early warning aspirating smoke detection system (VESDA) and addressable smoke detection system sense the presence of fire in the protected facility
- FM200firesuppressionsystem, which reaches extinguishing levels in10seconds or less, stopping ordinary combustion. It is delivered to distribution nozzles through a system piping network occupying whole data Center area, false floor void, room void & ceiling void.

Server Configuration:

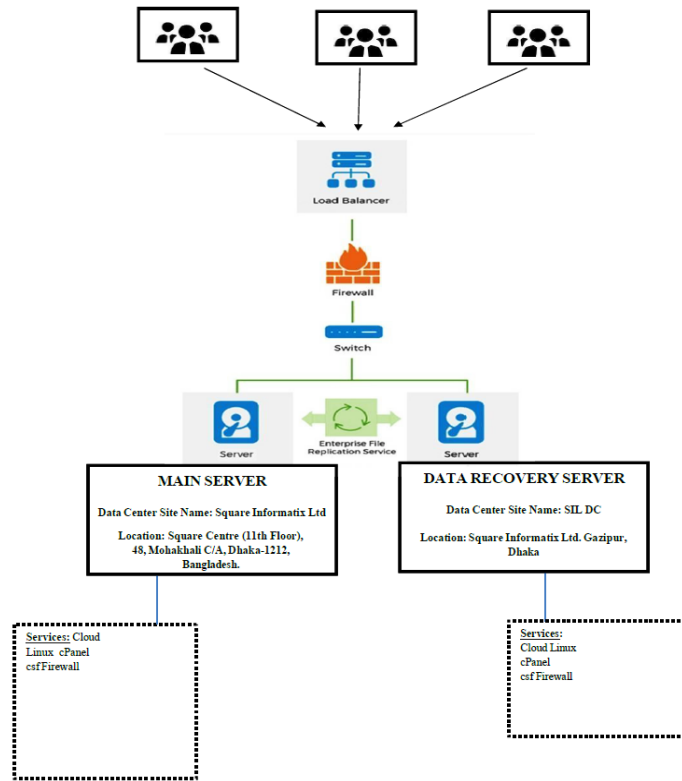
SN	Configuration Details
01	1 X Intel Xeon, Quad-Core
02	RAM: 16 GB SSD
03	HDD: 01 TB X 02 HDD
04	Connection: 10 MBPS, REAL IP: 01
05	Operating System: Cloud Linux
06	Platform: cPanel with necessary plugins
07	Power Backup Plan: Provided by Square Informatix Ltd.

Security and Firewall Details: ConfigServer Security & Firewall (csf)

Features of Firewall:

- Straight-forward SPI iptables firewall script
- Daemon process that checks for login authentication failures for:
 - Courier imap, Dovecot, uw-imap, Kerio
 - openSSH
 - cPanel, WHM, Webmail (cPanel servers only)
 - Pure-ftpd, vsftpd, Proftpd
 - Password protected web pages (htpasswd)
 - Mod_security failures (v1 and v2)
 - Suhosin failures
 - Exim SMTP AUTH
- Custom login failures with separate log file and regular expression matching
- POP3/IMAP login tracking to enforce logins per hour
- SSH login notification
- SU login notification
- Excessive connection blocking
- UI Integration for cPanel, DirectAdmin and Webmin
- Easy upgrade between versions from within cPanel/WHM, DirectAdmin or Webmin
- Easy upgrade between versions from shell
- Pre-configured to work on a cPanel server with all the standard cPanel ports open
- Pre-configured to work on a DirectAdmin server with all the standard DirectAdmin ports open
- Auto-configures the SSH port if it's non-standard on installation
- Block traffic on unused server IP addresses - helps reduce the risk to your server
- Alert when end-user scripts sending excessive emails per hour - for identifying spamming scripts
- Suspicious process reporting - reports potential exploits running on the server
- Excessive user processes reporting
- Excessive user process usage reporting and optional termination
- Suspicious file reporting - reports potential exploit files in /tmp and similar directories
- Directory and file watching - reports if a watched directory or a file changes
- Block traffic on a variety of Block Lists including DShield Block List and Spamhaus DROP List
- BOGON packet protection
- Pre-configured settings for Low, Medium or High firewall security (cPanel servers only)

- Works with multiple ethernet devices
- Server Security Check - Performs a basic security and settings check on the server (via cPanel/-DirectAdmin/Webmin UI)
- Allow Dynamic DNS IP addresses - always allow your IP address even if it changes whenever you connect to the internet
- Alert sent if server load average remains high for a specified length of time mod_security log reporting (if installed)
- Email relay tracking - tracks all email sent through the server and issues alerts for excessive usage (cPanel servers only)
- IDS (Intrusion Detection System) - the last line of detection alerts you to changes to system and application binaries
- SYN Flood protection
- Ping of death protection
- Port Scan tracking and blocking
- Permanent and Temporary (with TTL) IP blocking
- Exploit checks
- Account modification tracking - sends alerts if an account entry is modified, e.g. if the password is changed or the login shell
- Shared syslog aware
- Messenger Service - Allows you to redirect connection requests from blocked IP addresses to preconfigured text and html pages to inform the visitor that they have been blocked in the firewall. This can be particularly useful for those with a large user base and help process support requests more efficiently
- Country Code blocking - Allows you to deny or allow access by ISO Country Code
- Port Flooding Detection - Per IP, per Port connection flooding detection and mitigation to help block DOS attacks
- DirectAdmin UI integration
- Updated Webmin UI integration
- WHM root access notification (cPanel servers only)
- Ifd Clustering - allows IP address blocks to be automatically propagated around a group of servers running Ifd. It allows allows cluster-wide allows, removals and configuration changes
- Quick start csf - deferred startup by Ifd for servers with large block and/or allow lists
- Distributed Login Failure Attack detection
- Temporary IP allows (with TTL)
- IPv6 Support with ip6tables
- Integrated UI - no need for a separate Control Panel or Apache to use the csf configuration
- Integrated support for cse within the Integrated UI
- cPanel Reseller access to per reseller configurable options Unblock, Deny, Allow and Search IP address blocks
- System Statistics - Basic graphs showing the performance of the server, e.g. Load Averages, CPU Usage, Memory Usage, etc
- ipset support for large IP lists
- Integrated with the CloudFlare Firewall



DC-DR Plan Diagram

4.5 USER CAPACITY, TPS AND SESSION

High-load ready

Through our software Payment Wallet can process more than 300 transactions per second (TPS) without using expensive enterprise software or hardware. We route the transactions based on our algorithm set in our payment gateway software. When there is large number of transactions the algorithm automatically redirects to a free bank payment gateway to reduce heavy load.

Antifraud instruments

Our solution uses integrated checks and rules configuration for each payment transaction. Also can use popular scoring systems to ensure minimum fraud transactions level.

Fraud Detection Module

We have implemented the below fraud detection module that covers following features:

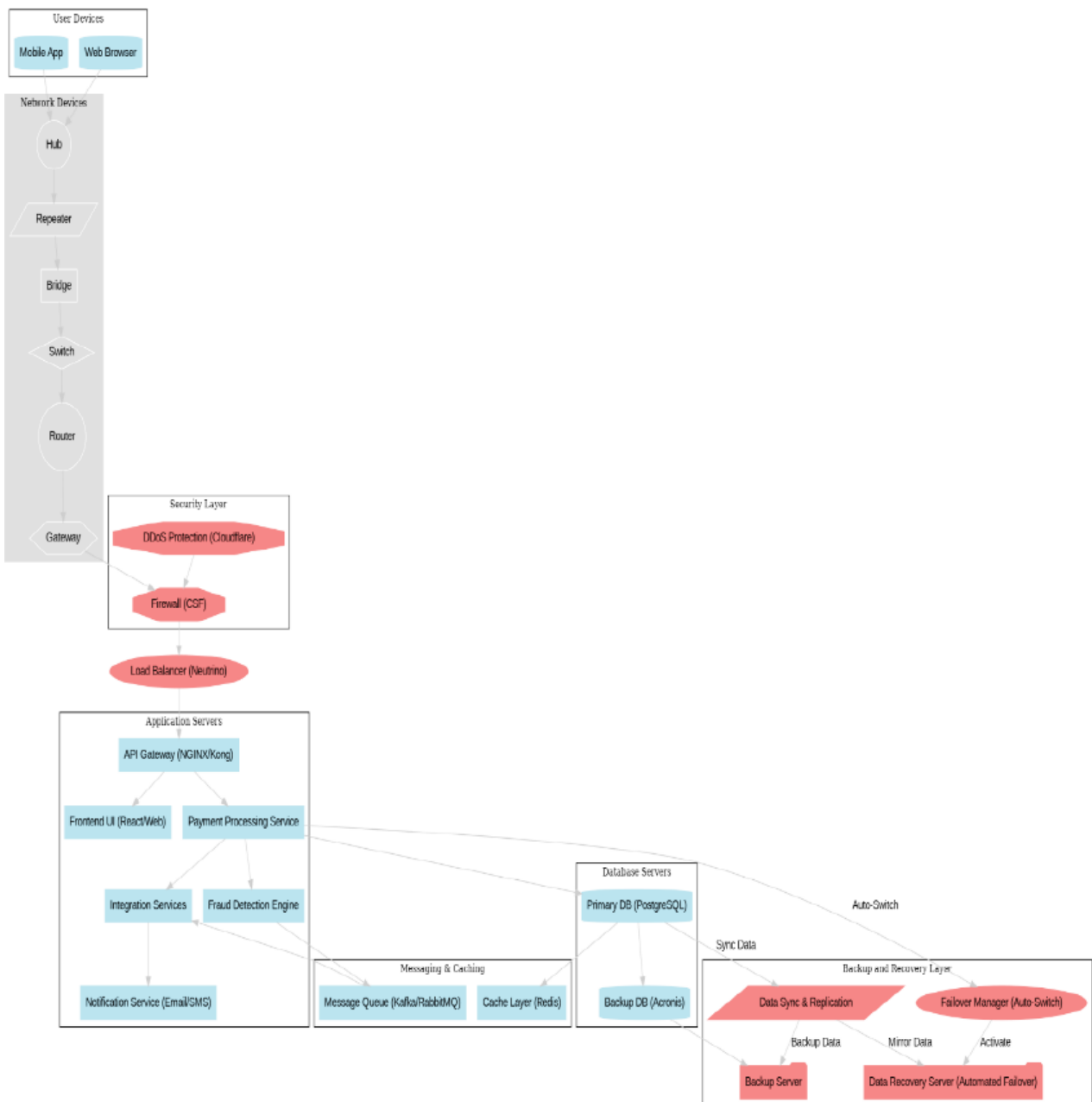
1. Card issuer country - Yes
2. Card issuer bank - Yes
3. 3D Secure Value Authentication successful - yes or no (depending on acquiring bank)
4. 3D Secure Value Authentication attempted - yes or no (depending on acquiring bank)
5. 3D Secure Value Authentication not attempted - yes or no (depending on acquiring bank)
6. Daily Maximum Times of Transactions by a single card - 3
7. Weekly Maximum Times of Transactions by a single card - 21
8. Monthly Maximum Times of Transactions by a single card - 90
9. Cardholder IP- Yes

Country of card issuance	3D Secure Value			Transaction Frequency		
	Authentication Successful (ECI: Visa 5, MC 2) yes or no	Authentication attempted (ECI: Visa 6, MC 1) yes or no	Authentication not attempted (ECI: Visa 7, MC 0) yes or no	Daily Maximum Times 3	Weekly Maximum Times 21	Monthly Maximum Times 90

Fault tolerance

We can provide different fault tolerance schemes, that depends upon our infrastructure.

5. Detailed network plan



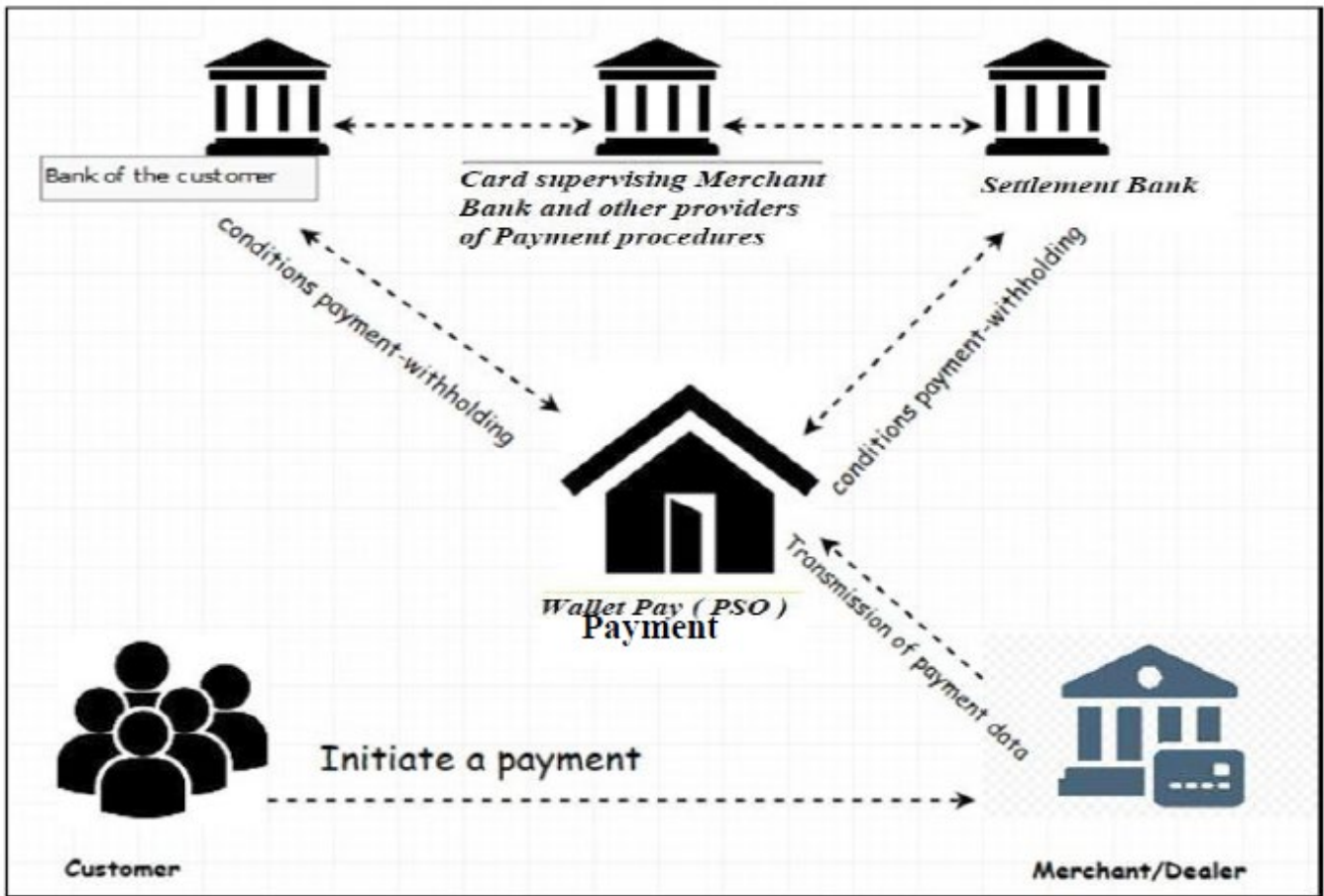


Diagram: Connectivity with the stakeholder

Several terms that are used almost interchangeably when describing online payments through PSO, all stakeholder functions are described below:

- Payment gateway
- Payment processor
- Payment provider
- Payment service or payment system
- Merchant account

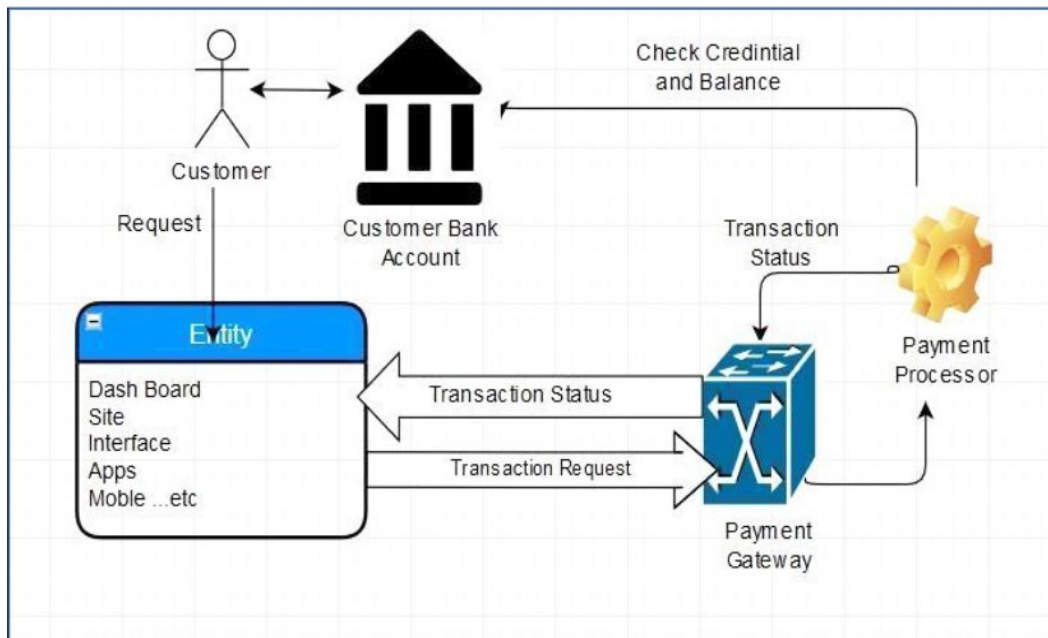
Each facilitates the completion of online transactions, and the processing of online payments.

a) Payment gateway

A payment gateway is a service that receives the online payment request from cloud/Web and directs it to the payment processor.

b) Payment processor

A payment processor is a service that validates the purchaser's card details and checks if they have sufficient funds in their account to cover the payment. If the customer has sufficient funds, the transaction is authorized, and the funds are transferred from the customer's account. The status of the transaction is transmitted back to the payment gateway which then sends a status message to website.



c) Payment operator

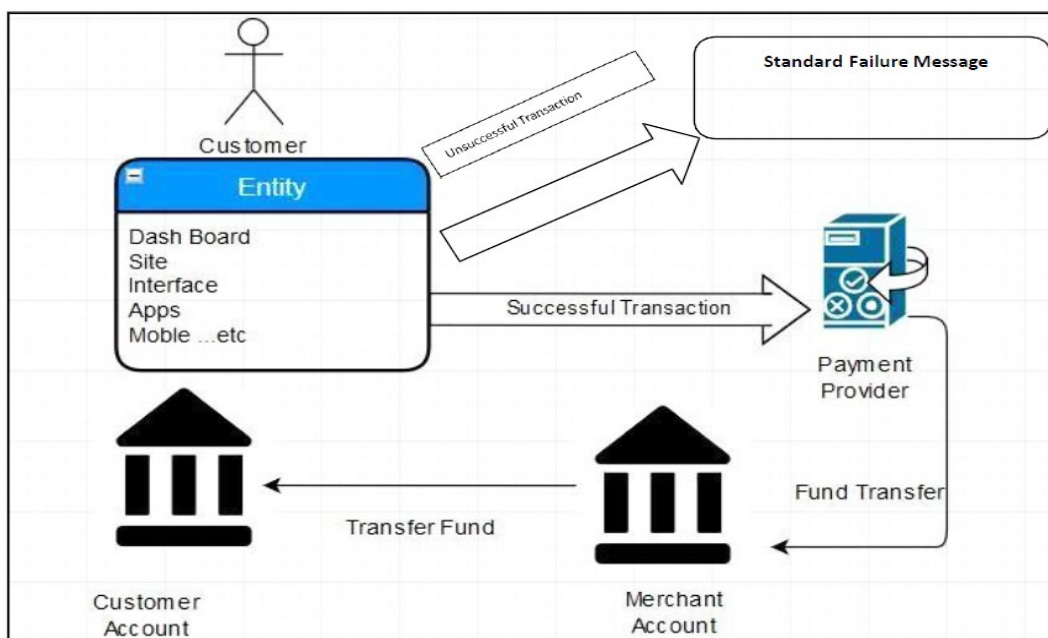
PSO is the company that operates the payment gateway or payment processor services. In some cases, the payment gateway and payment processor are combined into a single service known by either name.

d) Payment service or payment system

Where a payment provider offers multiple types of payment gateways – with different features and pricing – each type is referred to as a **payment service** or **payment system**.

e) Merchant account

When an online transaction is successfully completed, the funds are transferred from the purchaser's account to merchant account, a special kind of bank account used exclusively to hold funds received from credit and debit card transactions. To accept online payments, customer usually need to set up a merchant account with payment provider. Funds accumulating in your merchant account are transferred to customer bank account.



Data Center Site Facility:

5.1 Detailed Server Network Plan

Data Center Configuration and Details

Location: Square Informatix Ltd, Gazipur, Dhaka

SN	Description
01	Rack Space in Rack (600mm*1000mm)-Half Rack
02	POWER - AC Power with Generator back-up
03	Optical Fiber inside the exchange compound with ports and connectors in patch panel (ODF) at both ends
04	Bandwidth: 50 mbps
05	Media Converter (Including Power) - 2 Media Converter need for both end

Server Configuration:

SN	Configuration Details
01	Intel® Skylake i7-6700 Quad-Core, up to 4x 4.0 GHz
02	RAM: DDR4 32 GB
03	HDD: 2x 2TB SATA II HDD, 7,2k
04	Connection: 1 Gbit/s
05	Backup: Acronis Backup Basic
06	Operating System: Linux (CentOS)
07	Platform: cPanel/WHM

Power Backup Plan: Provided by SIL

Software/Platform Details: cPanel/WHM with necessary plugins

DDoS Protection: Cloudflare Protection

Load Balancer: Neutrino

Backup/Restore: CPREMOTE

- Can restore backup within 10 minutes,
- Recovery time depends on internet connection speed

[Security and Firewall Details: ConfigServer Security & Firewall \(csf\)](#)

Features of Firewall:

- Straight-forward SPI iptables firewall script
- Daemon process that checks for login authentication failures for:
 - Courier imap, Dovecot, uw-imap, Kerio
 - openSSH
 - cPanel, WHM, Webmail (cPanel servers only)
 - Pure-ftpd, vsftpd, Proftpd
 - Password protected web pages (htpasswd)
 - Mod_security failures (v1 and v2)
 - Suhosin failures
 - Exim SMTP AUTH
- Custom login failures with separate log file and regular expression matching
- POP3/IMAP login tracking to enforce logins per hour
- SSH login notification
- SU login notification
- Excessive connection blocking
- UI Integration for cPanel, DirectAdmin and Webmin
- Easy upgrade between versions from within cPanel/WHM, DirectAdmin or Webmin
- Easy upgrade between versions from shell
- Pre-configured to work on a cPanel server with all the standard cPanel ports open
- Pre-configured to work on a DirectAdmin server with all the standard DirectAdmin ports open
- Auto-configures the SSH port if it's non-standard on installation
- Block traffic on unused server IP addresses - helps reduce the risk to your server
- Alert when end-user scripts sending excessive emails per hour - for identifying spamming scripts
- Suspicious process reporting - reports potential exploits running on the server
- Excessive user processes reporting
- Excessive user process usage reporting and optional termination
- Suspicious file reporting - reports potential exploit files in /tmp and similar directories
- Directory and file watching - reports if a watched directory or a file changes
- Block traffic on a variety of Block Lists including DShield Block List and Spamhaus DROP List
- BOGON packet protection
- Pre-configured settings for Low, Medium or High firewall security (cPanel servers only)
- Works with multiple ethernet devices

- Server Security Check - Performs a basic security and settings check on the server (via cPanel/DirectAdmin/Webmin UI)
- Allow Dynamic DNS IP addresses - always allow your IP address even if it changes whenever you connect to the internet
- Alert sent if server load average remains high for a specified length of time
- mod_security log reporting (if installed)
- Email relay tracking - tracks all email sent through the server and issues alerts for excessive usage (cPanel servers only)
- IDS (Intrusion Detection System) - the last line of detection alerts you to changes to system and application binaries
- SYN Flood protection
- Ping of death protection
- Port Scan tracking and blocking
- Permanent and Temporary (with TTL) IP blocking
- Exploit checks
- Account modification tracking - sends alerts if an account entry is modified, e.g. if the password is changed or the login shell
- Shared syslog aware
- Messenger Service - Allows you to redirect connection requests from blocked IP addresses to preconfigured text and html pages to inform the visitor that they have been blocked in the firewall. This can be particularly useful for those with a large user base and help process support requests more efficiently
- Country Code blocking - Allows you to deny or allow access by ISO Country Code
- Port Flooding Detection - Per IP, per Port connection flooding detection and mitigation to help block DOS attacks
- DirectAdmin UI integration
- Updated Webmin UI integration
- WHM root access notification (cPanel servers only)
- lfd Clustering - allows IP address blocks to be automatically propagated around a group of servers running lfd. It allows allows cluster-wide allows, removals and configuration changes
- Quick start csf - deferred startup by lfd for servers with large block and/or allow lists
- Distributed Login Failure Attack detection
- Temporary IP allows (with TTL)
- IPv6 Support with ip6tables
- Integrated UI - no need for a separate Control Panel or Apache to use the csf configuration
- Integrated support for cse within the Integrated UI
- cPanel Reseller access to per reseller configurable options Unblock, Deny, Allow and Search IP address blocks
- System Statistics - Basic graphs showing the performance of the server, e.g. Load Averages, CPU Usage, Memory Usage, etc
- ipset support for large IP lists
- Integrated with the CloudFlare Firewall

How CPREMOTE works:

The screenshot shows the Cpremove Version 10.0 dashboard. The top navigation bar includes 'Dashboard', 'Accounts', 'Restore Backups', 'Preferences', 'Logs', and 'Help'. The main content area is divided into several sections:

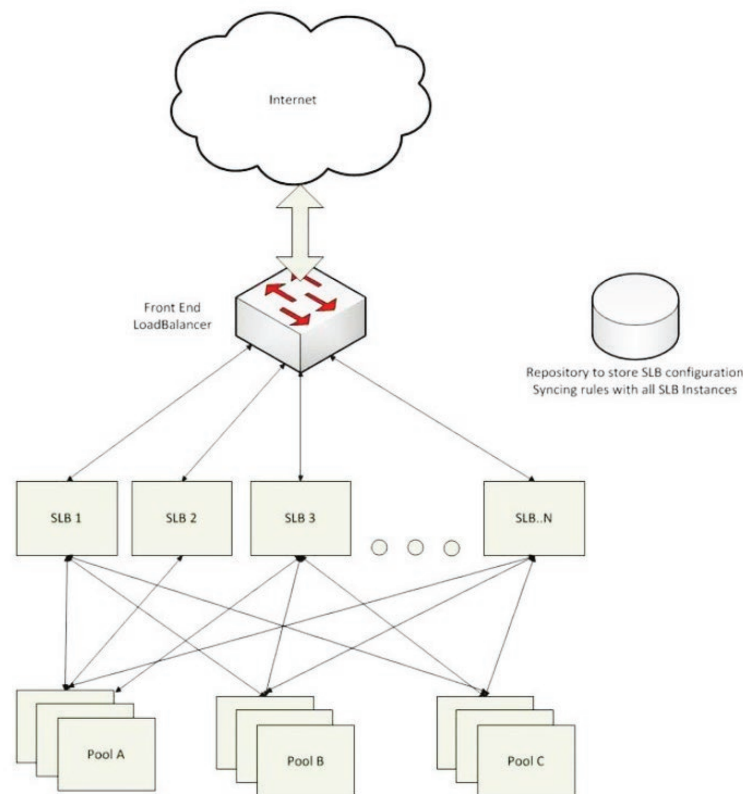
- Backup Domains:** A table with columns: S.No, Domain, User, Disk Usage, Backup Status. It lists 7 domains with their respective users and disk usage.
- Storage Pools:** A table with columns: S.No, Pool Name, Pool Type, Status. It lists 3 pools: 'ida' (Local Storage), 'desh' (Remote SSH), and 'v3' (Amazon S3).
- Backup Logs:** A table with columns: S.No, Log file, File Size, Date. It lists 3 log files with their sizes and dates.

At the bottom, there is a 'BACKUP ADMINISTRATION' bar with icons for: Cpremove Dashboard, Domain Restore, Database Restore, Email Restore, Restore My Home, File or Directory Restore, View Restore Logs, and Check Restore Progress.

Load Balancer Work Flow:

Neutrino is used by eBay and built using Scala & Netty. It supports least-connection and round- robin algorithms with the following switching features.

- Using canonical names
- Context-based
- L4 using TCP port numbers



Data Recovery Center Configuration and Details

Location: Square Centre (11th Floor), 48, Mohakhali C/A, Dhaka-1212, Bangladesh.

Server Configuration:

SN	Model	Description
01	Model	Dell PowerEdge R320 Server
02	Chassis Type	1-U Rack Mount
03	Processor	Intel Xeon E5-2407 v2 2.40GHz, 10M Cache, 6.4GT/s QPI, Turbo, 4C, 80W, Max Mem
04	No of processors	01 (One)
04	Chipset	Intel C600 Chipset
05	RAM	16GB Memory (2x8GB),RDIMM, 1600MT/s, Low Volt, Single Rank, x4 Data Width Up to 96GB (6 DIMM Slots)
06	Hard Drive	2 x 1TB 7.2K RPM NL-SAS, 6Gbps 3.5" Hot Plug Hard Drive
07	LAN /NIC	Integrated Dual Port 1GbE BASE-T
08	Remote Management	Baseboard Management Controller (12G)

Power Backup Plan: UPS (CyberPower) / Diesel Generator (Autostart)

Software/Platform Details: cPanel/WHM with necessary plugins

DDoS Protection: Cloudflare Protection

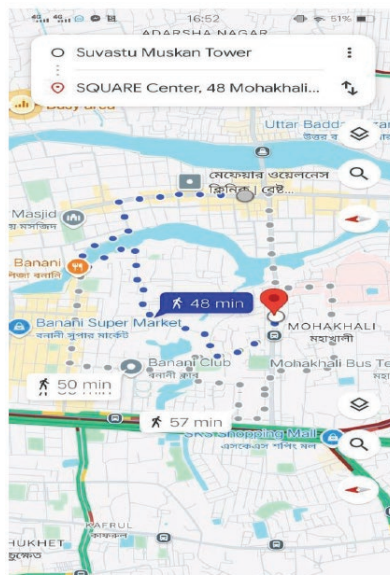
Load Balancer: Neutrino

Backup/Restore: CPREMOTE

- Can restore backup within 10 minutes,
- Recovery time depends on internet connection speed

Connectivity: Two dedicated fiber optic based connection from two separate reputed ISP with dedicated Real IP

Distance: The distance between SIL(Data Center Server) and Payment Wallet Office (Data Recovery Server) is showing more than 10 KM as shared by google maps screenshot below.



Security and Firewall Details: ConfigServer Security & Firewall (csf)

Features of Firewall:

- Straight-forward SPI iptables firewall script
- Daemon process that checks for login authentication failures for:
 - Courier imap, Dovecot, uw-imap, Kerio
 - openSSH
 - cPanel, WHM, Webmail (cPanel servers only)
 - Pure-ftpd, vsftpd, Proftpd
 - Password protected web pages (htpasswd)
 - Mod_security failures (v1 and v2)
 - Suhosin failures
 - Exim SMTP AUTH
 - Custom login failures with separate log file and regular expression matching
 - POP3/IMAP login tracking to enforce logins per hour
 - SSH login notification
 - SU login notification
- Excessive connection blocking
- UI Integration for cPanel, DirectAdmin and Webmin
- Easy upgrade between versions from within cPanel/WHM, DirectAdmin or Webmin
- Easy upgrade between versions from shell
- Pre-configured to work on a cPanel server with all the standard cPanel ports open
- Pre-configured to work on a DirectAdmin server with all the standard DirectAdmin ports open
- Auto-configures the SSH port if it's non-standard on installation
- Block traffic on unused server IP addresses - helps reduce the risk to your server
- Alert when end-user scripts sending excessive emails per hour - for identifying spamming scripts
- Suspicious process reporting - reports potential exploits running on the server
- Excessive user processes reporting
- Excessive user process usage reporting and optional termination
- Suspicious file reporting - reports potential exploit files in /tmp and similar directories
- Directory and file watching - reports if a watched directory or a file changes
- Block traffic on a variety of Block Lists including DShield Block List and Spamhaus DROP List
- BOGON packet protection
- Pre-configured settings for Low, Medium or High firewall security (cPanel servers only)
- Works with multiple ethernet devices
- Server Security Check - Performs a basic security and settings check on the server (via cPanel/DirectAdmin/Webmin UI)
- Allow Dynamic DNS IP addresses - always allow your IP address even if it changes whenever you connect to the internet

- Alert sent if server load average remains high for a specified length of time
- mod_security log reporting (if installed)
- Email relay tracking - tracks all email sent through the server and issues alerts for excessive usage (cPanel servers only)
- IDS (Intrusion Detection System) - the last line of detection alerts you to changes to system and application binaries
- SYN Flood protection
- Ping of death protection
- Port Scan tracking and blocking
- Permanent and Temporary (with TTL) IP blocking
- Exploit checks
- Account modification tracking - sends alerts if an account entry is modified, e.g. if the password is changed or the login shell
- Shared syslog aware
- Messenger Service - Allows you to redirect connection requests from blocked IP addresses to preconfigured text and html pages to inform the visitor that they have been blocked in the firewall. This can be particularly useful for those with a large user base and help process support requests more efficiently
- Country Code blocking - Allows you to deny or allow access by ISO Country Code
- Port Flooding Detection - Per IP, per Port connection flooding detection and mitigation to help block DOS attacks
- DirectAdmin UI integration
- Updated Webmin UI integration
- WHM root access notification (cPanel servers only)
- Ifd Clustering - allows IP address blocks to be automatically propagated around a group of servers running Ifd. It allows allows cluster-wide allows, removals and configuration changes
- Quick start csf - deferred startup by Ifd for servers with large block and/or allow lists
- Distributed Login Failure Attack detection
- Temporary IP allows (with TTL)
- IPv6 Support with ip6tables
- Integrated UI - no need for a separate Control Panel or Apache to use the csf configuration
- Integrated support for cse within the Integrated UI
- cPanel Reseller access to per reseller configurable options Unblock, Deny, Allow and Search IP address blocks
- System Statistics - Basic graphs showing the performance of the server, e.g. Load Averages, CPU Usage, Memory Usage, etc
- ipset support for large IP lists
- Integrated with the CloudFlare Firewall

How CPREMOTE works:

The screenshot displays the Cpremove Version 10.0 dashboard. At the top, it shows system information like 'CINTOS 7.3 x86_64 kun - cpdev WRM 62.0 (build 5) [DEV]' and 'Load Average: 0.11 0.04 0.05'. The main navigation bar includes 'Dashboard', 'Accounts', 'Restore Backups', 'Preferences', 'Logs', and 'Help'. The dashboard is divided into several sections:

- Backup Domains:** A table listing domains, users, disk usage, and backup status.

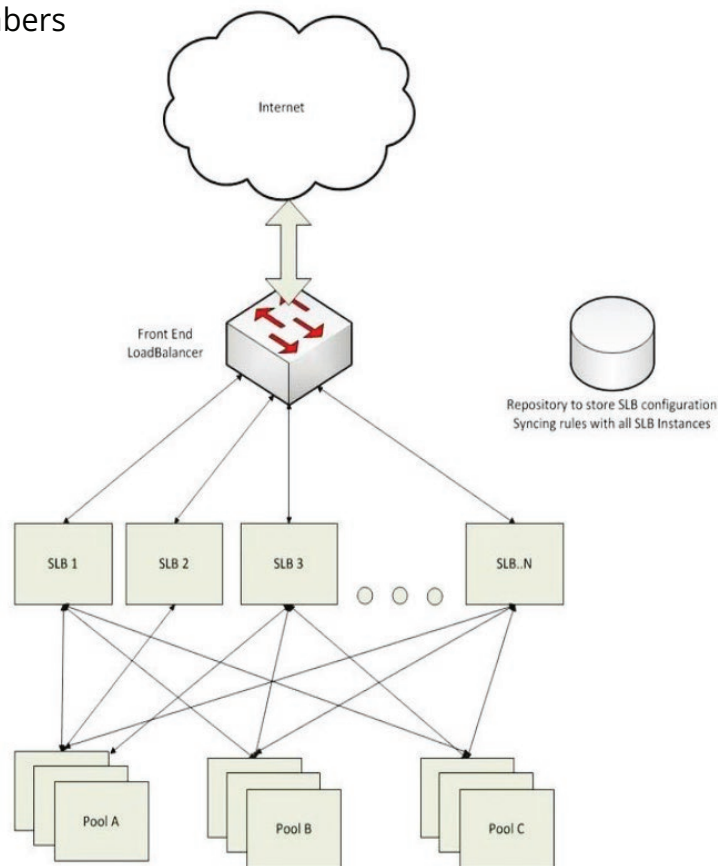
S.No	Domain	User	Disk Usage	Backup Status
1	angelberry.com	angelberry	2M	Enabled
2	arozza.com	arozza	6M	Enabled
3	avastars.com	avastars	0M	Enabled
4	avastars.com	avastars	1M	Enabled
5	brainconnection.com	brainconnection	1M	Enabled
6	cais.com	cais	1M	Enabled
7	cccc.com	cccc	3M	Enabled
- Storage Pools:** A table listing storage pools, their types, and status.

S.No	Pool Name	Pool Type	Status
1	sda	Local Storage	Active
2	clevish	Ramdisk SSH	Active
3	s3	Amazon S3	Active
- Backup Logs:** A table listing backup logs with columns for S.No, Log File, File Size, and Date.
- Backup Administration:** A navigation bar with icons for 'Cpremove Dashboard', 'Domain Restore', 'Database Restore', 'Email Restore', 'Restore My Home', 'File or Directory Restore', 'View Restore Logs', and 'Check Restore Progress'.

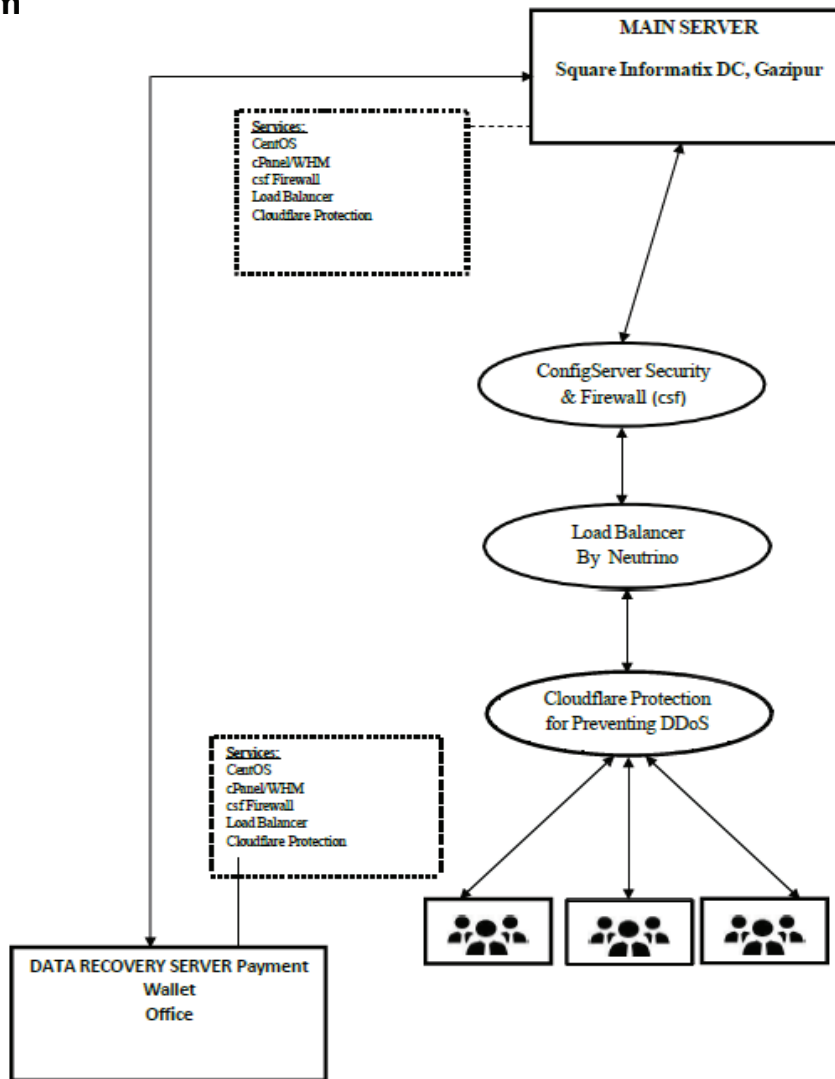
Load Balancer Work Flow:

Neutrino is used by eBay and built using Scala & Netty. It supports least-connection and round-robin algorithms with the following switching features.

- Using canonical names
- Context-based
- L4 using TCP port numbers



Plan Diagram



6. IT Risk Management process

IT risk is a component of the overall risk universe of an enterprise. Bank, NBF, PSP, PSO and every financial institution faces strategic risk, environmental risk, market risk, credit risk, operational risk, compliance risk, etc.

In many enterprises, IT related risk is considered to be a component of operational risk. However, even strategic risk can have an IT component itself, especially where IT is the key enabler of new business initiatives. The same applies for credit risk, where poor IT security can lead to lower credit ratings. It is better not to depict IT risk with a hierarchic dependency on one of the other risk categories. IT risk is business risk - specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within a Bank or NBF or PSP/PSO. It consists of IT related events and conditions that could potentially impact the business. It can occur with both uncertain frequency and magnitude and it creates challenges in meeting strategic goals and objectives.

ICT Risk Governance

As PSO Payment Wallet shall form an ICT Risk Management Committee to govern overall ICT risks and relevant mitigation measures. We shall define the Risk Appetite in terms of combinations of frequency and magnitude of a risk to absorb loss e.g., financial loss, reputation damage.

Payment Wallet shall define the Risk Tolerance (tolerable deviation from the level set by the risk appetite definition) having approval from the board/Risk Management Committee and clearly communicated to all stakeholders.

Payment Wallet shall review and approve risk appetite and tolerance change over time; especially for new technology, new organizational structure, new business strategy and other factors require the enterprise to reassess its risk portfolio at a regular interval. We shall define the risk responsibilities to individuals for ensuring successful completion. We shall define the risk accountability applies to those who owned the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific ICT Risk processes.

Ownership of risk stays with owner or custodian whoever is in better position to mitigate the identified risk for that specific ICT asset. We shall acknowledge all risks by Risk Awareness so that those are well understood and known and recognized as the means to manage them.

We shall contribute to executive management's understanding of the actual exposure to ICT risk by Open Communication, enabling definition of appropriate and informed risk responses.

We shall aware amongst all internal stakeholders of the importance of integrating risk and opportunity in their daily duties. We shall be transparent to external stakeholders regarding the actual level of risk and risk management processes in use.

We shall begin Risk-aware Culture from the top with board and executives, who set direction, communicate risk-aware decision making and reward effective risk management behaviors.

IT security department/unit/cell shall report status of identified ICT security risk to the ICT security committee and Risk Management Committee periodically as defined in the policy.

Meaningful IT risk assessments and risk-based decisions require ICT risks to be expressed in unambiguous and clear, business-relevant terms. Effective risk management requires mutual understanding between IT and the business over which risk needs to be managed. All stakeholders must have the ability to understand and express how adverse events may affect business objectives.

- A. An IT person shall understand how IT-related failures or events can impact enterprise objectives and cause direct or indirect loss to the enterprise.
- B. A business person shall understand how ICT-related failures or events can affect key services and processes.

Payment Wallet shall establish business impact analysis needs to understand the effects of adverse events. We may practice several techniques and options that can help them to describe IT risks in business terms. Payment Wallet shall practice the development and use of Risk Scenarios technique to identify the important and relevant risks amongst all. The developed risk scenarios can be used during risk analysis where frequency and impact of the scenario are assessed. We shall define Risk Factors those influence the frequency and/or business impact of risk scenarios. We shall interpret risk factors as casual factors of the scenario that is materializing, or as vulnerabilities or weaknesses.

IT security department/unit/cell shall conduct periodic ICT risk assessment of ICT related assets (process and system) and provide recommendation to risk owners for mitigation.

The ICT landscape is vulnerable to various forms of attacks. The frequency and malignancy of such attacks are increasing. It is imperative that Financial Institutions security solutions at the data, application, database, operating systems and networks to adequately address related threats. Appropriate measures shall be implemented to protect sensitive or confidential information such as customer personal information, account and transaction data which are stored and processed in systems. Customers shall be properly authenticated before access to online transactions, sensitive personal or account information.

The following measurements and security systems will be applied to mitigate the IT risk

6.1 Physical Security

- Physical security will be applied to the information processing area or Data Center. DC will be located in restricted area and unauthorized access shall be strictly prohibited.
- Only authorized staff can access to DC and only grant access to the DC on a need to have basis. Physical access of staff to the DC shall be revoked immediately if it is no longer required.
- Access authorization procedures shall be strictly applied to vendors, service providers, support staff and cleaning crews. Payment Wallet will ensure that visitors are accompanied at all times by an authorized employee while in the DC.
- Access authorization list shall be maintained and reviewed periodically for the authorized person to access the Data Center.
- All physical access to sensitive areas will be logged with purpose of access into the Data Center.
- Payment Wallet shall ensure that the perimeter of the DC, facility and equipment room are physically secured and monitored. Payment Wallet shall employ physical, human and procedural controls for 24 hours such as the use of security guards, card access system, mantraps and surveillance system where appropriate.
- Emergency exit door shall be available.

- Data Center will have a designated custodian or manager in charge to provide authorization and to ensure compliance with Policy.
- An inventory of all computing equipment, associated equipment and consumables housed in DC must be maintained by the manager or a delegate.
- In case DC is operated by an outsourced service supplier, there will be contract among the financial institutes, merchants and supplier and Payment Wallet will ensure that all the requirements of Policy regarding physical security must be complied with and that the Bank or NBFi reserves the right to review physical security status at any time.
- If DC is operated by an outsourced service supplier, the responsibility for physical security lies with the supplier, but access to such facilities dedicated to bank use must be reviewed and authorized by the Bank or NBFi.
- The physical security of Data Center premises shall be reviewed at least once each year.

6.2 Data Security

Processing payments and handling private personal data require cumbersome certifications. Personal and payment data breaches are getting larger and more common.

Online transaction can be risky business as technology advances and electronic theft becomes more complex. Payment Wallet will comply with PCI-compliant e-commerce credit card & online payment processing services, security features and advanced fraud management tools to keep your business, your customers and your data safe from fraud. To secure customers data Payment Wallet will follow the Guideline on ICT Security for Banks and NBFi. As guided by Bangladesh bank cryptography will be implemented to protect Data. The primary application of cryptography is to protect the integrity and privacy of sensitive or confidential information. Cryptography is commonly used in Banks and NBFis to protect sensitive customer information such as PINs relating to critical applications (e.g. ATMs, payment cards and online financial systems).

All encryption algorithms used in a cryptographic solution shall depend only on the secrecy of the key and not on the secrecy of the algorithm. As such, the most important aspect of data encryption is the protection and secrecy of cryptographic keys used, whether they are master keys, key encrypting keys or data encrypting keys.

Payment Wallet shall establish cryptographic key management policy and procedures covering generation, distribution, installation, renewal, revocation and expiry. Payment Wallet shall ensure that cryptographic keys are securely generated. All materials used in the generation process shall be destroyed after usage and ensure that no single individual knows any key in its entirety or has access to all the constituents making up these keys. Cryptographic keys shall be used for a single purpose to reduce the impact of an exposure of a key.

The effective timeframe that a cryptographic key may be used in a given cryptographic solution is called the crypto period. Payment Wallet shall define the appropriate crypto period for each cryptographic key considering sensitivity of data and operational criticality.

Payment Wallet shall ensure that hardware security modules and keying materials are physically and logically protected. When cryptographic keys are being used or transmitted, we shall ensure that these keys are not exposed during usage and transmission. When cryptographic keys have expired, we shall use a secure key destruction method to ensure keys could not be recovered by any parties.

In the event of changing a cryptographic key, we shall generate the new key independently from the previous key.

Payment Wallet shall maintain a backup of cryptographic keys. The same level of protection as the original cryptographic keys shall be accorded to backup keys. If a key is compromised, we shall immediately revoke, destroy and replace the key and all keys encrypted under or derived from the exposed key. We will shall inform all parties concerned of the revocation of the compromised keys.

6.3 Operational Security

Payment Wallet shall establish appropriate security monitoring systems and processes, to facilitate prompt detection of unauthorized or malicious activities by internal and external parties.

We shall implement network surveillance and security monitoring procedures with the use of network security devices, such as intrusion detection and prevention systems, to protect the Bank or NBF I against network intrusion attacks as well as provide alerts when an intrusion occurs.

We may implement security monitoring tools which enable the detection of changes to critical ICT resources such as databases, system or data files and programs, to facilitate the identification of unauthorized changes.

We shall regularly review security logs of systems, applications and network devices for anomalies. Logs shall be protected and retained for defined period to facilitate future investigation.

We will implement some real life physical security so that our daily operation will not hamper. The people who will be involved with the system have a good background so that Payment Wallet and customers will not face any difficulties for their daily operation. Different level of RFID based physical access control will be implemented in workplace. In some valid cases 2-step verification for logging into system with access log will be implemented. Other standard HR policy to protect company in disaster situation caused by key person involved with the system will be applied too.

6.5.1 User Access Management

Payment Wallet shall only grant user access to ICT systems and networks on a need-to-use basis and within the period when the access is required. We shall closely monitor non-employees (contractual, outsourced, or vendor staff) for access restrictions. Each user must have a unique User ID and a valid password. User ID Maintenance form with access privileges shall be duly approved by the appropriate authority. User access shall be locked for unsuccessful login attempts.

User access privileges must be kept updated for job status changes. Payment Wallet shall ensure that records of user access are uniquely identified and logged for audit and review purposes.

We shall perform regular reviews of user access privileges to verify that privileges are granted appropriately.

6.6 Others

6.6.1 Password Management

Payment Wallet shall enforce strong password controls over users' access. Password controls shall include a change of password upon first logon. Password definition parameters shall ensure that minimum password length is maintained according to Bank's Policy (at least 6 characters).

Password shall be combination of at least three of stated criteria like uppercase, lowercase, special characters and numbers.

Maximum validity period of password shall not be beyond the number of days permitted in the Bank's Policy (maximum 90 days' cycle). Parameter to control maximum number of invalid logon attempts shall be specified properly in the system according to the Bank's Policy (maximum 3 consecutive times).

Password history maintenance shall be enabled in the system to allow same passwords to be used again after at least three (3) times. Administrative passwords of Operating System, Database and Business Applications shall be kept in a safe custody with sealed envelope.

6.6.2 Input Control

Session time-out period for users shall be set in accordance with the specified Policy.

Operating time schedule of users' input for banking applications shall be implemented as per regulatory enforcement unless otherwise permitted from appropriate authority.

Audit trail with User ID and date-time stamp shall be maintained for data insertion, deletion and modification. Software shall not allow the same user to be both maker and checker of the same transaction unless otherwise permitted from appropriate authority. Management approval must be in place for delegation of authority. Sensitive data and fields of banking applications shall be restricted from being accessed.

6.6.3 Privileged Access Management

Information security ultimately relies on trusting a small group of skilled staff, who shall be subject to proper checks and balances. Their duties and access to systems resources shall be placed under close scrutiny. Payment Wallet shall apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions. Having privileged access, all system administrators, ICT security officers, programmers and employees performing critical operations invariably possess the capability to inflict severe damage on critical systems. We shall adopt following controls and security practices for privileged users:

- A. Implement strong authentication mechanisms
- B. Implement strong controls over remote access
- C. Restrict the number of privileged users
- D. Grant privileged access on a “need-to-have” basis
- E. Review privileged users’ activities on a timely basis
- F. Prohibit sharing of privileged accounts
- G. Disallow vendors from gaining privileged access to systems without close supervision and monitoring

6.6.4 Internet Access Management

Internet access shall be provided to employees according to the approved Internet Access Management Policy. Access to and use of the internet from bank premises must be secure and must not compromise information security of Bank or NBF. Access to the Internet from bank premises and systems must be routed through secure gateways.

Any local connection directly to the Internet from Bank or NBF premises or systems, including standalone PCs and laptops, is prohibited unless approved by Information Security.

Employees shall be prohibited from establishing their own connection to the Internet using banks’ systems or premises. Use of locally attached modems with banks’ systems in order to establish a connection with the Internet or any third-party or public network via broadband, ISDN or PSTN services is prohibited unless specifically approved.

Internet access provided by the Bank or NBF must not be used to transact any commercial business activity that is not done by the Bank or NBF. Personal business interests of staff or other personnel must not be conducted.

Internet access provided by the Bank or NBF must not be used to engage in any activity that knowingly contravenes any criminal or civil law or act. Any such activity will result in disciplinary action of the personnel involved.

All applications and systems that require connections to the Internet or third-party and public networks must undergo a formal risk analysis during development and before production use and all required security mechanisms must be implemented.

6.6.5 Email Management

Email system shall be used according to the Bank's or NBF's or any financial policy.

- Access to email system shall only be obtained through official request. Email shall not be used to communicate confidential information to external parties unless encrypted using approved encryption facilities.
- Employees must consider the confidentiality and sensitivity of all email content, before forwarding email or replying to external parties.
- Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of the Bank or NBF, or contain any material that is harmful to employees, customers, competitors, or others. The willful transmission of any such material is likely to result in disciplinary action.
- Email system is principally provided for business purposes. Personal use of the bank email system is only allowed under management discretion and requires proper permission such personal use may be withdrawn or restricted at any time.
- Corporate email address must not be used for any social networking, blogs, groups, forums, etc. unless having management approval.
- Email transmissions from the Bank or NBF must have a disclaimer stating about confidentiality of the email content and asking intended recipient.
- Concerned department shall perform regular review and monitoring of email services.

6.6.6 Vulnerability Assessment and Penetration Testing

Vulnerability assessment (VA) is the process of identifying, assessing and discovering security vulnerabilities in a system.

Payment Wallet shall conduct VAs regularly to detect security vulnerabilities in the ICT environment. We shall deploy a combination of automated tools and manual techniques to perform a comprehensive VA. For web-based systems, the scope of VA shall include common web vulnerabilities such as SQL injection, cross-site scripting, etc.

We shall establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed. We shall carry out penetration tests in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system. Payment Wallet shall conduct penetration tests on network infrastructure and internet-based systems periodically or need basis.

6.6.7 Patch Management

Payment Wallet shall establish and ensure that the patch management procedures include identification, categorization and prioritization of security patches. To implement security patches in a timely manner, we shall establish the implementation timeframe for each category of security patches.

Payment Wallet shall perform rigorous testing of security patches before deployment into the production environment.

7. Business Continuity and Disaster Recovery Plan

Business Continuity and Disaster Recovery Plan is required for planning of business resiliency for critical incidents, operational risks take into account for wide area disasters, Data Center disasters and the recovery plan. The primary objective of Business Continuity Plan (BCP) is to enable a Bank or NBFIs or any Financial Institute to survive in a disaster and to re-establish normal business operations. In order to survive with minimum financial and reputational loss, Bank or NBFIs shall assure that critical operations can resume normal processing within a reasonable time frame. The contingency plan shall cover the business resumption planning and disaster recovery planning. Contingency plan shall also address the backup, recovery and restore process.

7.1 Business Continuity Plan (BCP)

Payment Wallet will have an approved Business Continuity Plan addressing the recovery from disaster to continue its operation. Approved BCP shall be circulated to all relevant stakeholders. The recipients would receive a copy of amended plan whenever any amendment or alteration takes place.

- A. Documents related to BCP must be kept in a secured off-site location. One copy shall be stored in the office for ready reference.
- B. The BCP shall be coordinated with and supported by the Business Impact Analysis (BIA) and the Disaster Recovery Plan (DRP) considering system requirements, processes and interdependencies.

BCP shall address the followings:

- A. Action plan to restore business operations within the specified time frame for: i) office hour disaster ii) outside office hour disaster.
- B. Emergency contacts, addresses and phone numbers of employees, vendors and agencies.
- C. Grab list of items such as backup tapes, laptops, flash drives, etc.
- D. Disaster recovery site map

BCP must be tested and reviewed at least once a year to ensure the effectiveness.

7.1.1 Disaster Recovery Plan (DRP)

Payment Wallet must have an approved Disaster Recovery Plan. In formulating and constructing a rapid recovery plan, the Bank or NBFIs or financial institute shall include a scenario analysis to identify and address various types of contingency scenarios. Payment Wallet shall consider scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents as well as a total incapacitation of the primary DC.

- A. Payment Wallet will establish a Disaster Recovery Site (DRS) which is geographically separated from the primary site (minimum of 10 kilometers radial distance but choice of different seismic zone will be preferred) to enable the restoration of critical systems and resumption of business operations when a disruption occurs at the primary site.
- B. If Disaster Recovery Site (DRS) is not in different seismic zone, Bank or NBFIs may establish a third site in different seismic zone which will be treated as Disaster Recovery Site (DRS)/Far DC. In such case the DRS in near location will be treated as Near DC and shall be configured accordingly.
- C. DRS and/or Near DC shall be equipped with compatible hardware and telecommunication equipment to support the critical services of the business operation in the event of a disaster.
- D. Physical and environmental security of the DRS and/or Near DC shall be maintained.
- E. Payment Wallet shall define system recovery and business resumption priorities and establish specific recovery objectives including recovery time objective (RTO) and recovery point objective (RPO) for ICT systems and applications. RTO is the duration of time, from the point of disruption, within which a system shall be restored. RPO refers to the acceptable amount of data loss for an ICT system while a disaster occurs.
- F. Payment Wallet shall consider inter-dependencies between critical systems in drawing up its recovery plan and conducting contingency tests.
- G. Payment Wallet may explore recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance the bank's recovery capability.
- H. Information security shall be maintained properly throughout the recovery process.
- I. An up-to-date and tested copy of the DR plan shall be securely held off-site. One copy shall be stored in the office for ready reference.
- J. We shall test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.
- K. We shall involve its business users in the design and execution of comprehensive test cases to verify that recovered systems function properly.
- L. DR test documentation shall include at a minimum of Scope, Plan and Test Result. Test report shall be communicated to management and other stakeholders and preserved for future necessity.

7.1.2 Data Backup and Restore Management

PSO shall develop a data backup and recovery policy. Each business application must have a planned, scheduled and documented backup strategy, involving the making of both on- and off-line backups and the transfer of backups to secure off-site storage.

- A. Details of the planned backup schedule for each business application must be created in line with the classification of the application and the information it supports and must specify the type of back-up required (full, partial, incremental, differential, real-time monitoring) at each point in the back-up schedule.
- B. The frequency of backups taken for information must be determined in line with the classification of the information and the requirements of the business continuity plans for each application.
- C. The details of the planned backup schedule for each business application must include the retention period for backed-up or archived information and the retention period must be consistent with local legal and regulatory requirements.
- D. All media contained backed-up information must be labeled with the information content, backup cycle, backup serial identifier, backup date and classification of the information content.
- E. The backup inventory and log sheet shall be maintained, checked and signed by the supervisor.
- F. The Bank or NBFIs or PSO/PSP shall encrypt backup data in tapes or disks, containing sensitive or confidential information, before transported offsite for storage.
- G. At least one copy of backup shall be kept on-site for the time critical delivery.
- H. The process of restoring information from both on- and off-site backup storage must be documented.
- I. PSO shall carry out periodic testing and validation of the recovery capability of backup media and assess whether it is adequate and sufficiently effective to support the bank's recovery process.

7.1.3 Data Recovery Center Configuration and Details

Data Recovery Center Configuration and Details

Data Recovery Site Name: SIL

Location: Square Centre (11th Floor),48, Mohakhali C/A, Dhaka-1212, Bangladesh.

Data Recovery Site facility:

- 10,000 SQF stat of the art data center facility.
- 180 COLD AISLE CONTAINMENT RACKs capacity.
- N+N redundant UPS in every datacenter for uptime
- Automated Multiple Redundant diesel generators
- Dual power PDU in each rack
- Power racks ranging from 4KW to10KW
- Datacenter suite available for collocation services
- Metered PDU for rack level power monitoring and billing
- Redundant Air-Conditioned DC Environment
- N+1 precision air conditioner to maintain 20+/-1°C temperature and 50+/-5% relative humidity
- Cold aisle containments are implemented in two rows, containments are fabricated in stronger aluminum frames & Acrylic sheets
- Use of vermiculite material for green solution datacenter
- Fire-Protected Facility
- The highly advance laser based very early warning aspirating smoke detection system (VESDA) and addressable smoke detection system sense the presence of fire in the protected facility
- FM200firesuppressionsystem, which reaches extinguishing levels in10seconds or less, stopping ordinary combustion. It is delivered to distribution nozzles through a system piping network occupying whole data Center area, false floor void, room void & ceiling void.

Server Configuration:

SN	Configuration Details
01	1 X Intel Xeon, Quad-Core
02	RAM: 16 GB SSD
03	HDD: 01 TB X 02 HDD
04	Connection: 10 MBPS, REAL IP: 01
05	Operating System: Cloud Linux
06	Platform: cPanel with necessary plugins
07	Power Backup Plan: Provided by SIL

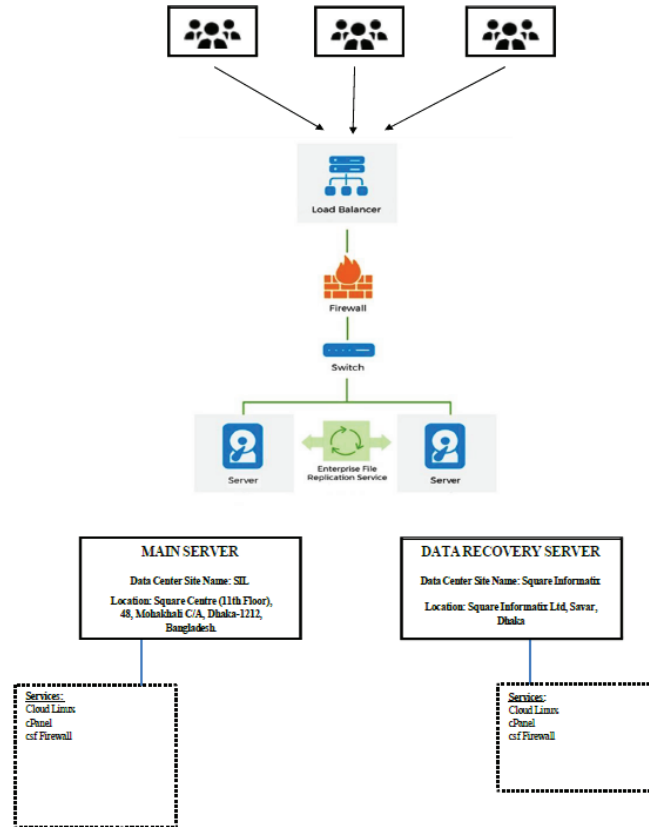
Security and Firewall Details: ConfigServer Security & Firewall (csf)

Features of Firewall:

- Straight-forward SPI iptables firewall script
- Daemon process that checks for login authentication failures for:
 - Courier imap, Dovecot, uw-imap, Kerio
 - openSSH
 - cPanel, WHM, Webmail (cPanel servers only)
 - Pure-ftpd, vsftpd, Proftpd
 - Password protected web pages (htpasswd)
 - Mod_security failures (v1 and v2)
 - Suhosin failures
 - Exim SMTP AUTH
- Custom login failures with separate log file and regular expression matching
- POP3/IMAP login tracking to enforce logins per hour
- SSH login notification
- SU login notification
- Excessive connection blocking
- UI Integration for cPanel, DirectAdmin and Webmin
- Easy upgrade between versions from within cPanel/WHM, DirectAdmin or Webmin
- Easy upgrade between versions from shell
- Pre-configured to work on a cPanel server with all the standard cPanel ports open
- Pre-configured to work on a DirectAdmin server with all the standard DirectAdmin ports open
- Auto-configures the SSH port if it's non-standard on installation
- Block traffic on unused server IP addresses - helps reduce the risk to your server
- Alert when end-user scripts sending excessive emails per hour - for identifying spamming scripts
- Suspicious process reporting - reports potential exploits running on the server
- Excessive user processes reporting
- Excessive user process usage reporting and optional termination
- Suspicious file reporting - reports potential exploit files in /tmp and similar directories
- Directory and file watching - reports if a watched directory or a file changes
- Block traffic on a variety of Block Lists including DShield Block List and Spamhaus DROP List
- BOGON packet protection
- Pre-configured settings for Low, Medium or High firewall security (cPanel servers only)
- Works with multiple ethernet devices
- Server Security Check - Performs a basic security and settings check on the server (via cPanel/DirectAdmin/Webmin UI)
- Allow Dynamic DNS IP addresses - always allow your IP address even if it changes whenever you connect to the internet

- Alert sent if server load average remains high for a specified length of time
- mod_security log reporting (if installed)
- Email relay tracking - tracks all email sent through the server and issues alerts for excessive usage (cPanel servers only)
- IDS (Intrusion Detection System) - the last line of detection alerts you to changes to system and application binaries
- SYN Flood protection
- Ping of death protection
- Port Scan tracking and blocking
- Permanent and Temporary (with TTL) IP blocking
- Exploit checks
- Account modification tracking - sends alerts if an account entry is modified, e.g. if the password is changed or the login shell
- Shared syslog aware
- Messenger Service - Allows you to redirect connection requests from blocked IP addresses to preconfigured text and html pages to inform the visitor that they have been blocked in the firewall. This can be particularly useful for those with a large user base and help process support requests more efficiently
- Country Code blocking - Allows you to deny or allow access by ISO Country Code
- Port Flooding Detection - Per IP, per Port connection flooding detection and mitigation to help block DOS attacks
- DirectAdmin UI integration
- Updated Webmin UI integration
- WHM root access notification (cPanel servers only)
- lfd Clustering - allows IP address blocks to be automatically propagated around a group of servers running lfd. It allows allows cluster-wide allows, removals and configuration changes
- Quick start csf - deferred startup by lfd for servers with large block and/or allow lists
- Distributed Login Failure Attack detection
- Temporary IP allows (with TTL)
- IPv6 Support with iptables
- Integrated UI - no need for a separate Control Panel or Apache to use the csf configuration
- Integrated support for cse within the Integrated UI
- cPanel Reseller access to per reseller configurable options Unblock, Deny, Allow and
- Search IP address blocks
- System Statistics - Basic graphs showing the performance of the server, e.g. Load Averages, CPU Usage, Memory Usage, etc
- ipset support for large IP lists
- Integrated with the CloudFlare Firewall

DC- DR Plan Diagram



8. Settlement, REVERSAL AND DISPUTE management process

A dispute resolution committee will be formed by this payment wallet, this committee will work to resolve any types of disputes in a speedy, efficient and quick manner. Perhaps, a dedicated Payment System Committee can be established to not only act as dispute settlement body (empowered with administrative), but also acts as an oversight committee to represent the stakeholders and to supervise the progress and the development of the company. The committee, further made up of interested parties from the Association of Payment System Providers and other interest groups and stakeholders in the industries could ensure certain guidelines or protocol to be set out in further details to ensure transparency, clarity and fairness to all stakeholders. We hope, whilst not full proof in itself and still work in progress, would cut bureaucracy to a certain extent.

CONSUMER PROTECTION & ANTI-MONEY LAUNDERING MEASURES

This is important as uninformed and uneducated customers are actually relying much on the trust between the involved parties in the transaction and putting their money to those who they have never seen before. Therefore, the Government may need to start to put effort to overcome the apparent gap existing due to the unavailability of any legal instrument / protections by customers which is becoming more apparent in recent times; either by issuing other legal instruments as a follow up according to the Regulation, adding other provisions, or issuing policy to ensure the unexpected damage (loss of transactions) occurred may be prevented.

The Government will require to address the issues of consumer protection in terms of their transaction and investments. The flexibility of financial transaction facilitated through the internet platform which is accessible to any internet user is obviously a threat to the uninformed, non-sophisticated "man on the streets". Whilst we are aware it is difficult to police the proliferation of any investment (local or foreign) schemes, a task force within the white-collar crime of the police unit will be a good start including working alongside with security experts. Phishing, scamming, and others type of threat in Internet are only name to few. Under the veil of the activities of financial transaction there lies a greater risk of the platform being used as a white-collar crime. Money laundering, corruption, and name of any other financial crime can easily flow through such transactions in a form of layering to cover the result of the crime committed, and in the process, innocent investors may be duped into thinking that they are investing in a legitimate vehicle.

Anti-Money Laundering and Combating of Financing of Terrorism (AML/CFT) laws, however, those law lack some muscles in that the law does not address the development of financial technology in providing legal remedies for white collar crimes. As important principle requiring financial institution to check up the background of its customer must be prepared to endure the development of technology, especially when it comes to the cross-border transaction. As it is obviously inevitable to prevent any cross-border transaction, any individual may easily be conducting any financial transaction, including payment transaction. Therefore, safeguards need to be in place to provide safe and secure system to the development of financial technology.

Setting up of a Payment Wallet Fintech Office

In order to ensure the strength of the financial payment system and monitor the progress of the well-being of the industry players, the setting up of a Fintech office is in the right direction. The Office can be tasked with the overall strategic setting process, setting policies in relation to governance and control of payment systems to ensure the logical and lawful payment system.

Building blocks of Payment Wallet for an Adequate Resolution plan



POLICY AND DECISION MAKING

Our resolution plan will include following four elements with detail descriptions

- i. The pursued objective of resolution
- ii. A description of possible resolution scenarios, e.g. merger or liquidation
- iii. The bodies, functions and individuals authorized to take the decision to resolve the company, the decision making process, and the stakeholders involved
- iv. The manner in which decisions are recorded and documented, to enable stakeholders to verify afterwards whether the resolution process was performed ethically and orderly

For each scenario, Payment Wallet will identify verifiable triggers that may prompt the management board to consider resolution. The relationship between the trigger and the final decision to resolve the disputes and all the decisions will be transparent and verifiable for all stakeholders.

RISK ANALYSIS

As part of compiling a resolution plan, we are obliged to perform a risk analysis of the resolution process. The resolution plan will include a list of the main operational risks that may occur during the resolution process and may put the objective of the plan (orderly resolution in the interest of all payment service users) in danger. Payment Wallet will translate the outcome of our risk and then analysis into procedures and measures to mitigate the identified risks. Resolution plan also include a procedure for monitoring the development of risks and mitigating measures, e.g. as part of the periodic evaluation process of the resolution plan.

GOVERNANCE

The continuity of management must be guaranteed during the entire resolution process. In order to achieve this, the Payment Wallet management board put guarantees in place that there will be sufficient people and resources to continue services and at the same time execute the resolution process in an orderly fashion. Our resolution plan must contain the company's governance structure during resolution, including a rough description of the roles and responsibilities of the project organization. Payment Wallet resolution will clearly describe the professionalism and expertise necessary for orderly resolution.

OPERATIONAL ASPECTS

Resolution plan will include a realistic project plan describing the steps that are necessary to resolve the company, promptly, appropriately and fully, distinguishing between

- i. The processes and tasks that must be performed in order to guarantee orderly resolution, and the individuals responsible for those tasks, and
- ii. (Realistic) time lines, milestones and dependencies

FINANCIAL ASPECTS

Obeying the laws and regulation Payment Wallet will form a Resolution that will clearly describe how the financial resolution of liabilities has been arranged for all entitled parties, ensuring that all claims are transferred orderly (fully and well-balanced) and that any amounts charged are reasonable and fair.

Secondly, resolution will also provide a rough estimate of the financial resources necessary for each scenario. Payment Wallet ensure to Bangladesh Bank that we will have sufficient certainty that the necessary financial resources for each scenario.

And thirdly, plan include a description of how financial risks and costs will be approached.

Additional Document

ICT Security Policy.

Corporate Office: Suvastu Muskan Tower

(7th floor)

56 Gulshan Avenue, Gulshan 1

Dhaka-1212, Bangladesh.

“This Policy is Ltd (CRAFT CODE LTD) property and intended for the internal use of CRAFT CODE LTD only. The recipient should ensure that this document is not reproduced outside of CRAFT CODE LTD without the prior approval of the owner.”

| Confidentiality Notice |

This policy is confidential and contains proprietary information and intellectual property of CRAFT CODE LTD. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of the CRAFT CODE LTD. Please be aware that disclosure, copying, distribution, or use of this document and the information contained therein is strictly prohibited and the CRAFT CODE LTD shall be taken disciplinary action against such violation of the policy.

| Review frequency |

This policy shall be reviewed annually and upon significant change to the organization.

| Enforcement |

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

DOCUMENT INFORMATION:

Area	Description
Document Name:	ICT Security Policy
Document Version	Version 1.0
Document Reference	CRAFT CODE LTD/DOC/POLICY/001
Document Type	Policy & Guidelines
Document Classification	Sensitive
Effective Date	September 15 ,2024
Owner	Craft Code Ltd
Custodian	Craft Code Ltd

REVISION HISTORY :

Version	Date	Revision Author	Summary of Changes
N/A			

Note: As this is the first version of the document, there is no revision history.

DISTRIBUTION :

Name	Title
CRAFT CODE LTD	All Staff of the CRAFT CODE LTD.

PROPOSER :

Proposer	Title	Date	Signature
Colin Patra Managing Director & CEO	ICT Security Policy	August 11,2024	

DOCUMENT CONTROL

TITLE	Network Security Policy.	Effective Date: 11.08.2024
DOCUMENT ID	CRAFT CODE LTD/DOC/POL/0001	Version: 1.0 Page 7 to 17

1. Network Security Policy

1.1. Purpose

Network security and management in Information and Communication Technology (ICT) is the ability to maintain the integrity of a system or network, its data, and its immediate environment. Networks systems play a critical part in the day-to-day business operation of CRAFT CODE LTD Limited. Networks not only connect many of the components of business processes internally but also link the organization with its valuable customers, stakeholders, and remittance hub all over the globe, as a result, the intruder would try to steal sensitive information and disrupt CRAFT CODE LTD service and business activities. Therefore, the network needs to be protected to ensure that the confidentiality, integrity, and availability of CRAFT CODE LTD services for the customer.

The effective protection of our networks requires that we adopt industry-accepted best practices in information security covering the design, implementation, operation, and management. We have to ensure that everyone involved follows these practices. Sources of industry-accepted practices include, but are not limited to:

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST)

1.2. Scope

This policy sets out Craft Code Ltd.'s rules and standards for network protection and acts as a guide for those who create and maintain our IT infrastructure. Its intended audience is IT and information security management, and support staff who will implement and maintain the organization's defense This control applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, customers, and other third parties who have access to CRAFT CODE LTD systems.

Network Security Policy

1.2.1. Network security design

Network security design is the process of designing a network so that it includes measures that prevent internal and extranet threats and minimize risk factors along with ensuring Confidentiality, Integrity, and availability. We impose security controls based on a specific set of business requirements. This policy does not attempt to specify how individual networks should be designed and built but guides the standard building blocks that should be used.

1.2.2. Requirements

A network must be based on a clear definition of requirements which should include the following security-related factors:

- The classification of the information to be carried across the network.
- A risk assessment of the potential threats to the network and vulnerability assessment.
- Encryptions shall be maintained with network components and partner organizations.
- The agreement maintains for an hour of availability and degree of resilience with the Service provider (ISP).
- The security controls are in place and maintained strictly.

1.2.3. Policy statement

The network security policy is intended to protect the integrity of CRAFT CODE LTD networks, mitigate the risks and losses associated with security threats. Network security management ensures the security arrangement with various rules and procedures that only authorized users may be able to obtain access.

1.2.3.1. CRAFT CODE LTD establish baseline standards to ensure security for network equipment.

1.2.3.2. Different security zones (e.g. MZ, DMZ, and Test Zone, etc.) define in network design and security configurations shall be implemented under a documented plan.

1.2.3.3. Cable security shall be implemented including UTP, Optical fiber cable, and Power for further corrective or preventive maintenance work.

1.2.3.4. Network equipment shall be ensured through physical security.

1.2.3.5. IT LAN shall be segregated where required.

1.2.3.6. Sensitive data/information shall be traveled in the entire network through encrypted or otherwise protected channels. [WAN or Public Network].

1.2.3.7. To protect network perimeters Next-Generation Firewall with Intrusion Prevention System (IPS) must be installed within internal networks to minimize the impact of security exposures originating from third-party or overseas systems, as well as trusted Networks.

1.2.3.8. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH (Secure Shell) or IP Sec (IP Security)).

1.2.3.9. Security admins review the firewall rules quarterly and remove not relevant rules with proper documentation.

1.2.3.10. CRAFT CODE LTD's shall establish redundant communication links for WAN connectivity.

1.2.3.11. CRAFT CODE LTD's deploying Wireless Local Area Network (WLAN) shall be aware of risks associated with this environment. In the case of Wireless network shall be encrypted with AP to Mobile device communication and it will be a separate network with MAC address bindings.

1.2.3.12. Rectification log for critical Network Device Syslog server shall be implemented and the log will be analyzed regularly.

- 1.2.3.13. Managing network devices (Router and Switch) access AAA server shall be implemented.
- 1.2.3.14. Role-based access control lists shall be implemented in the router to control network traffic.
- 1.2.3.15. A bandwidth monitoring tool may be implemented for surveillance of all network equipment and servers.
- 1.2.3.16. The connection of personal laptops to the office network or any personal wireless modem with the office laptop/desktop is discouraged.
- 1.2.3.17. The unused Switch port must be disabled or shut down.
- 1.2.3.18. Integration of any new connection or service with the existing network of the CRAFT CODE LTD, to justify and validate the requirements, the respective service stakeholder shall share necessary documents to the network team to classify information that will be passed and accessed through.
- 1.2.3.19. CRAFT CODE LTD shall maintain IPsec VPN Secure channel different partner to enhance data security and this network traffic shall pass through Next Generation firewall which enhances extra layer of protection among the network.
- 1.2.3.20. The CRAFT CODE LTD network team shall periodically monitor all network connectivity with network monitoring tools.
- 1.2.3.21. CRAFT CODE LTD connects different geographical locations such as Branch, Corporate Head office, Data Center, Disaster Recovery Center and far disaster recovery site using Wide Area Network (WAN) topology through the encrypted mechanism.
- 1.2.3.22. CRAFT CODE LTD shall implement security controls such ACL, IPS, DDOS attack protection, blocking suspicious traffic and geo-location filter, allowing specific port and protocol for running services at both perimeter and Server farm Firewall.
- 1.2.3.23. CRAFT CODE LTD shall deploy web applications firewall to enhance web service security like SQL injections, code-base attack, sensitive data exposure, broken access controls, cross-site scripting (XSS), and insecure deserializations.
- 1.2.3.24. CRAFT CODE LTD shall be implemented endpoint solutions for workstation & server.
- 1.2.3.25. The CRAFT CODE LTD shall maintain proper documentation before deploying or integrations any new service in the existing network.

1.3. Public/Untrusted Network

To ensure secure data transmission over the public network CRAFT CODE LTD shall maintain public certifications like SSL v3.0 or TLS 1.2 or higher version deployed as ensured data integrity and confidentiality.

1.3.1. The CRAFT CODE LTD shall be using TLS 1.2 or a higher version for the untrusted network.

1.3.2. The CRAFT CODE LTD shall maintain separate encryptions profile and symmetric key or IPsec peerkey for the partner network device integrations.

1.3.3. The public certificate shall be used for internet-based application systems which have been published publically.

1.3.4. The CRAFT CODE LTD must be restricted internet browsing for the end-user and maintain a separate form for internet access.

1.3.5. The CRAFT CODE LTD shall be monitoring all the internet user activities and publish reports quarterly through SOC meetings.

1.4. Wireless Networks

Wireless technology provides a convenient mechanism for accessing user resources. These technologies have become ubiquitous in the workplace environment. The advent of wireless technologies adds increased functionality but also adds security risks and concerns that must be managed and mitigated.

Wireless networks are comparatively limited in speed, bandwidth, and coverage to wired networks. Where possible, the use of a wired connection is preferred because it is faster and does not compete with other wireless devices for bandwidth. However, the use of wireless devices is increasing as it provides a convenient mechanism for accessing resources. Along with this convenience is a need for managed security as the devices are natively less secure than a hardwired device. The following procedures and practices shall be implemented to reduce risks related to wireless networks:

1.4.1. Older encryption protocols such as wired equivalent privacy (WEP) or SSL are not used for authentication or transmission.

1.4.2. Wireless networks transmitting sensitive information or connected to sensitive information environments, use industry best practices to implement strong encryption for authentication and transmission.

1.4.3. Wireless networks must be secured using WPA2 encryption or 802.1X Authenticated Wireless Access.

1.4.4. Processes test for the presence of rogue wireless access points and detect and identify all authorized and unauthorized wireless access points in premises.

1.4.5. The CRAFT CODE LTD shall maintain different segmented networks and control access through a firewall for the Wireless user.

1.4.6. Disable Wireless SSID broadcast for CRAFT CODE LTD internal network.

1.4.7. The CRAFT CODE LTD must be carried out to scan for the presence of wireless access points and detect and identify all authorized and unauthorized wireless access points quarterly. If unauthorized wireless access points are detected the Security Incident Response Procedure will be invoked immediately.

1.4.8. CRAFT CODE LTD has maintained secure and restricted wireless connectivity by ensuring MAC address binding with specific static IP addresses and maintaining strong access controls through the firewall for access CRAFT CODE LTD services.

1.4.9. CRAFT CODE LTD shall maintain separate (Physical) internet access for the guest user, BYOD, and external vendors through wireless media, and CRAFT CODE LTD maintain Static IP address and MAC for the users.

1.4.10. Any wireless access points considered to be in the organization's Cardholder Data Environment (CDE) will be recorded in the CDE Asset Inventory.

1.5. Physical Security

The objective is to prevent unauthorized physical access, damage, theft, compromise of assets, and interference to the sensitive area and information, and interruption of critical activities.

1.5.1. Visitors (Guest/Vendor representatives) may be allowed to access the data center with the proper notification of IT and ADC Ops Division.

1.5.2. The data center's access shall be allowed for authorized staff, and the other will be allowed to access on a need to have.

1.5.3. Access authorized list to be maintained, and to be updated as and when required which will be approved by HOIT.

1.5.4. Security guards and security alerts shall be engaged/installed for 24 hours in the data center. Data Centre's should be under CCTV coverage.

1.5.5. Log register to be maintained with reasons of access with date and time while visiting the data Centre.

1.5.6. Power supply and network connectivity shall be documented and physical security shall be reviewed every year.

1.5.7. IT equipment (Like the server, switch, router) inventory of the Data Centre should be properly maintained under the supervision of a manager or concerned person.

1.5.8. Backbone and centralized network equipment must be housed in appropriate lockable cabinets or racks in a secure server room to which only authorized support staff to have access (except for local facilities staff for reasons of health and safety).

1.5.9. Wireless access points located in public areas must be hidden from view where possible and should be placed in positions where access by the public is difficult e.g. in or near

1.5.10. the ceiling. A lockable protective casing must be installed where an access point is in an unprotected public area e.g. a car park.

1.5.11. Physical and/or logical controls must be implemented to restrict access to publicly accessible network ports on office walls. For example, network ports located in public areas and areas accessible to visitors must be disabled and only enabled when network access is explicitly authorized.

1.5.12. Any components considered to be within the Cardholder Data Environment must be subject to frequent tamper testing to ensure the devices have not been compromised. Staff members will be trained to inspect devices for tampering and record their findings in the CDE Asset Inventory.

1.5.13. The CRAFT CODE LTD shall shut down all unused switch ports and configure the access controls list for remote access.

1.5.14. The CRAFT CODE LTD shall enable port-security control of all the switching environments.

1.5.15. Components within the Cardholder Data Environment (CDE) is regularly tested whether it has been tampered with or not by trained staff. The test report is then recorded in the asset inventory for future decisions/use.

1.6. Remote Access

A remote access policy is a written document containing the guidelines for connecting to an organization's network from outside the office and below are the following controls are:

1.6.1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to internal networks.

1.6.2. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel.

1.6.3. VPN gateways will be set up and managed by network management of IT and ADC Ops Division.

1.6.4. All computers connected to internal networks via VPN or any other technology must use the most up-to-date anti-virus software.

1.6.5. VPN users will be automatically disconnected from the network after 30 minutes of inactivity.

1.6.6. Multi-factor authentication must be used on the client side.

1.6.7. Network Access Control (NAC) must be used to restrict access to remote clients.

1.6.8. Privilege access management (PAM) control must be used during the accessing service from a remote site.

1.6.9. The CRAFT CODE LTD shall use SSL VPN with Multiple factors like OTP for further authentications

1.6.10. VPN user request from approving by the Head of Department (HOD) and it came through VPN request form and it must be approved by the Security team and Head of IT (HOIT).

1.7. Network Security Incidents

An incident occurs when an attack, or other violation of your security policy, is carried out against the system, and unexpected disruptions occur for the systems which will badly hamper CRAFT CODE LTD services.

1.7.1. Events may lead to being security incidents recorded and managed according to the Information Security Incident Response Procedure.

1.7.2. The CRAFT CODE LTD has designated a cybersecurity incident response team - sometimes called a computer incident response team (CIRT), which will respond accordingly for the ICT-related incident.

1.8. Security Testing

A fundamental part of network security and vulnerability management is the ability to test and verify the strength of the organization's security controls against ever-changing cyber threats. The results of security testing must be risk assessed and applied to the treatment process to remediate any vulnerabilities found. Please refer to the Technical Vulnerability Management Policy and Risk Assessment and Treatment Process for more information.

1.8.1. IT systems (Operating System, Network Device, and Application) must undergo periodic perform Vulnerability Assessment and penetration testing.

1.8.2. In the VA process, CRAFT CODE's shall be deploying a combination of automated tools and manual [Popular Source/Trusted Source] technic to perform a comprehensive VA.

1.8.3. CRAFT CODE LTD shall be checked common attacks like SQL Injection, Password Cracking, and Man in the Middle attack, Session Hijacking, etc.

1.8.4. After gap analysis (Perform VAs), CRAFT CODE LTD should take initiative to remediate those vulnerabilities based on severity.

1.8.5. The CRAFT CODE LTD shall conduct penetration tests on IT systems periodically or need basis.

1.8.6. CRAFT CODE LTD maintains remediation and conducted risk assessment and documented risk treatment process.

DOCUMENT CONTROL		
TITLE	Cryptographic Policy.	Effective Date: 11.08.2024
DOCUMENT ID	CRAFT CODE LTD /DOC/POL/0002	Version: 1.0 Page 15 to 22

2. Cryptographic Policy

2.1. Purpose

The purpose of this policy is to protect the confidentiality, integrity, and privacy of sensitive or confidential information of CRAFT CODE Ltd. This policy protects sensitive customer information such as Account Number, PAN, transmission data, applications data, PINs, that have related to critical applications (e.g. ATM's, payment cards and online financial transactions, e-commerce transactions, etc.) of CRAFT CODE LTD. Encryptions ensured data confidentiality and integrity to keep information's secret for the unauthorized person.

A key component in the set of controls available to organizations to protect their classified information is the use of cryptographic techniques to "scramble" information so that it cannot be accessed without knowledge of a key.

Cryptographic controls are used to achieve several information security-related objectives, including:

- Confidentiality – ensuring that information cannot be read by unauthorized persons.
- Integrity – proving that data has not been altered in transit or whilst stored.
- Authentication – proving the identity of an entity requesting access to resources.
- Non-repudiation – proving that an event did or did not occur or that a message was sent by an individual.

2.2. Scope

This policy covers appropriate rules and use of cryptography for CRAFT CODE LTD Ltd covering generations, distributions, installations, renewal, revocation, and expiry. Cryptography can be used to protect the confidentiality of data, such as financial or personal data, whether that data is in storage or transit. These techniques are critical to the development and use of national and global information and communications networks and technologies, as well as the development of electronic commerce. This policy will ensure that no sophisticated information will pass outside of the CRAFT CODE LTD network without proper justifications as well as proper authorizations.

2.3. Policy Objectives

The objectives of this policy with regards to the protection of information system resources against the violations of confidentiality and integrity from unauthorized access are to:

2.3.1. Minimizing the threat of accidental, unauthorized, or inappropriate access to critical or sensitive electronic information owned by the CRAFT CODE LTD or temporarily entrusted to the parties for applying/deploying an equal level of encryption or encryption keys.

2.3.2. Enhance CRAFT CODE LTD security as well as ensure confidentiality and integrity of the information system resources which may lead to compromise CRAFT CODE LTD private and publically exposed resources.

2.3.3. Safeguard of the reputations of the CRAFT CODE LTD which may lead to loss, disclosure, or corruption of critical or sensitive information.

2.3.4. Using cryptographic techniques to authenticate users and other system entities requesting access or transacting with system users, entities, and resources.

2.4. Policy on the use of cryptographic controls

CRAFT CODE LTD used cryptographic techniques to control data security from internal and external threat sources, and managed approach as follows: -

2.4.1. Implementations Areas

Requirements for the use of cryptographic techniques will be identified and prepared risk mitigation plan, according to discovery services where cryptographic techniques must be applied to achieve the level of protection needed. In addition, cryptography will generally be implemented by default in the following scenarios:

2.4.1.1. Data in Use, data at rest, and data in motion.

2.4.1.2. Communication channel, media, gateway, or any transmission areas.

2.4.1.3. For authorized use of removable media such as USB memory sticks.

2.4.1.4. API, Applications, Database, Network transmission, PIN generation, etc.

2.4.1.5. Compliance, regulations, and laws.

2.4.1.6. Transactional systems shall be deployed PKI certificate (SSL standard certificate or EV). (* Not to the limited.)

2.4.2. Deployment

The deployment of cryptographic techniques must be managed carefully to ensure that the desired level of security is achieved. During the deployment of the cryptographic architecture, more than one member of staff is assigned to avoid a single point of failure for support and to allow segregations of duties to take place.

2.4.2.1. During the deployment, all implemented documents must be maintained by the CRAFT CODE LTD personal.

2.4.2.2. For smooth operations, CRAFT CODE LTD personal must be prepared operational procedure documents and educate the relevant staff for troubleshooting.

2.4.3. Testing and Review

After successfully deployed, CRAFT CODE LTD personal must be tested, where the encryption is properly working and able to encrypt/decrypt the network traffic between the site, and the globe.

2.5. Policy Statement

The primary application of cryptography is to protect the integrity and privacy of sensitive or confidential information. Cryptography is commonly used in CRAFT CODE LTD to protect sensitive customer information such as Passwords, PINs, sessions relating to critical applications (e.g. ATMs, payment cards and online financial systems, e-commerce transactions), and communication between Branches to the core network or remote access for support.

2.5.1. Cryptographic keys used for PIN encryption/decryption and related key management shall be created using processes to ensure encryptions that it is not possible to predict any key as well as decryptions key without the original key.

2.5.2. Cryptographic keys shall be generated in security way and immediately destroy all materials encryption after use or key generation process.

2.5.3. Cryptographic keys may be used for a single or multipurpose purpose.

2.5.4. CRAFT CODE LTD shall ensure that keys are conveyed or transmitted securely, CRAFT CODE LTD shall establish controls to ensure key loading to hosts and PIN entry device is handled securely.

2.5.5. The CRAFT CODE LTD will be defined as the appropriate crypto period for each cryptographic key considering sensitivity of data and operational criticality and key lifetime shall be deferred case to case.

2.5.6. The CRAFT CODE LTD will ensure that Hardware/Software security modules and keying materials are physically and logically protected, and the CRAFT CODE LTD will ensure that the SSL/TLS key/certificate will be protected logically.

2.5.7. When cryptographic keys are being used or transmitted, the CRAFT CODE LTD will be ensured that these keys are not exposed during usage and transmission.

2.5.8. When cryptographic keys have expired, the CRAFT CODE LTD will use a secure key destruction process to ensure keys could not be recovered by any parties.

2.5.9. The CRAFT CODE LTD will maintain a backup of cryptographic keys. The same level of protection as the original cryptographic keys will be accorded to backup keys.

2.5.10. In case of key is compromised, CRAFT CODE LTD will immediately revoke, destroy, and replace the key and all keys encrypted under or derived from the exposed key. CRAFT CODE LTD will inform all the parties of the repeal of the compromised keys.

2.6. Payment Card Data Protection

2.6.1. Sensitive authentication data must not be stored after authorization, even if encrypted. If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

2.6.2. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:

- Business justification and
- Data is stored securely.

2.6.3. Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.

2.6.4. Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography, (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures.

2.6.5. PAN must be rendered unreadable or secured with strong cryptography whenever it is sent via end- user messaging technologies.

2.7. Cryptographic Architecture

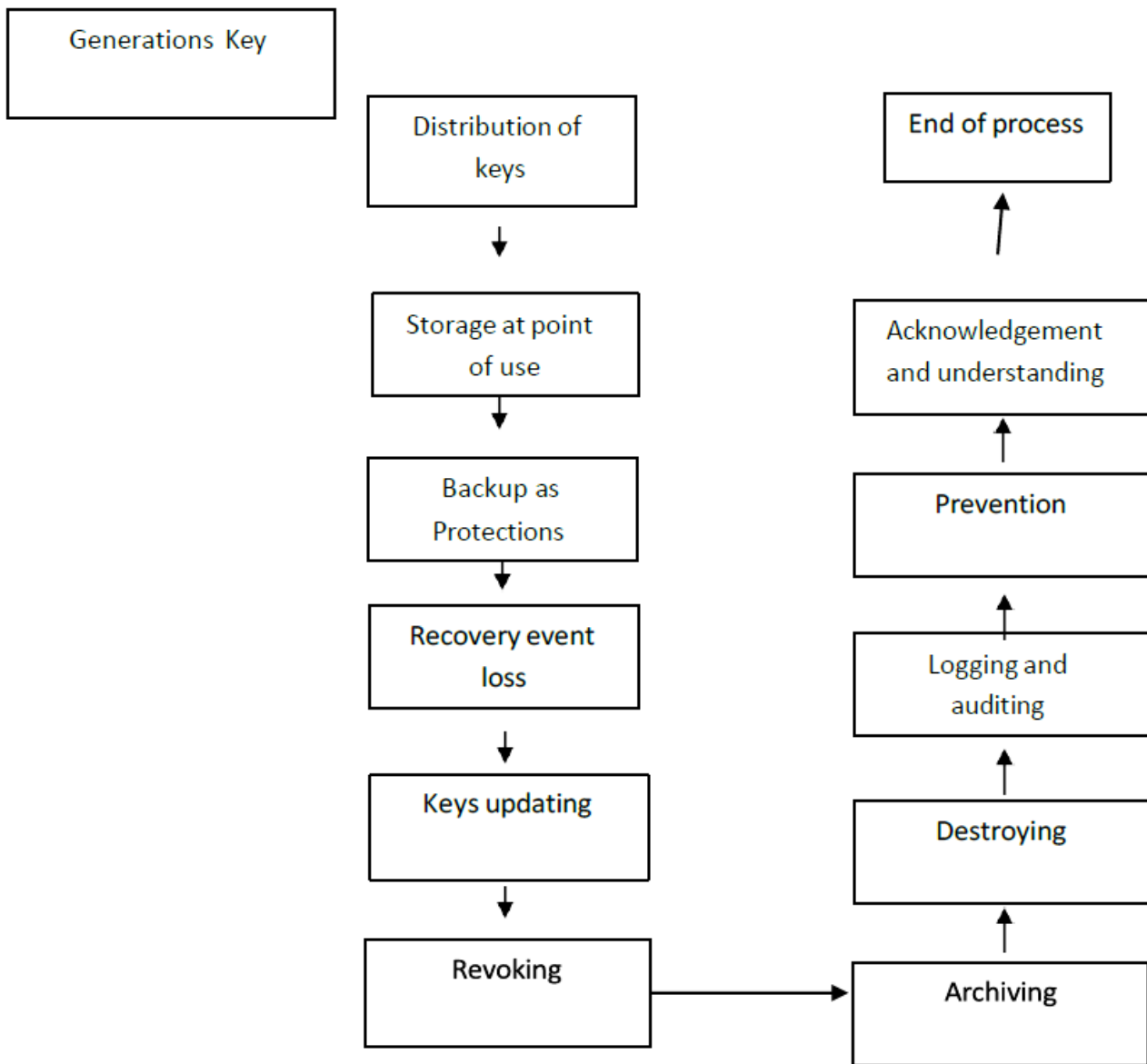
Below is a table that lists all the cryptographic architectures used in CRAFT CODE LTD.

KEY USAGE	ALGORITHMS, PROTOCOLS, AND KEYS USED	KEY STRENGTH	KEY EXPIRY	HARDWARE SECURITY MODULE (HSM)	SECURE CRYPTOGRAPHIC DEVICE (SCD) USED
Encrypting the PAN	AES-256	2048-bit	July 2025	Encryption Hardware	N/A
Taking card payments	AES-256	2048-bit	July 2025	N/A	P2PE chip and PIN device.

2.8. Key management Process

Cryptographic keys are stored and protected from modification, loss, destruction, and unauthorized disclosure. The following controls must be in place to protect the keys:

- Access to keys must be restricted to the fewest number of custodians.
- Key-encrypting keys must be at least as strong as the data-encrypting keys they protect.
- Keys must be stored securely in the fewest possible locations and forms.
- Lifecycle Approach must be taken to key management which will require the creation of specific procedures to cover the following stages.



2.8.1. Key control Cycle

The key management life cycle leads to key generations, transmission, process, key store, revoke and destroy, and the CRAFT CODE LTD maintains sufficient controls to meet its business requirements.

2.8.1.1. Key Generation:

The first stage for any key is always Key Generation, where the symmetric key or asymmetric key pair is created.

2.8.1.1.1. The CRAFT CODE LTD shall ensure that cryptographic keys are securely generated. Proper Inspection must be ensured prior to era (i.e. Ensure no electronic tapping tool, entire seclusion, no visual or digital surveillance, no need of multi-purpose computing structures).

2.8.1.1.2. Cryptographic keys or Key pairs shall be generated in accordance with the standard specifies, under the common public-key cryptographic techniques by the appropriate Approved by the global standard.

2.8.1. Key control Cycle

The key management life cycle leads to key generations, transmission, process, key store, revoke and destroy, and the CRAFT CODE LTD maintains sufficient controls to meet its business requirements.

2.8.1.1. Key Generation:

The first stage for any key is always Key Generation, where the symmetric key or asymmetric key pair is created.

2.8.1.1.1. The CRAFT CODE LTD shall ensure that cryptographic keys are securely generated. Proper Inspection must be ensured prior to era (i.e. Ensure no electronic tapping tool, entire seclusion, no visual or digital surveillance, no need of multi-purpose computing structures).

2.8.1.1.2. Cryptographic keys or Key pairs shall be generated in accordance with the standard specifies, under the common public-key cryptographic techniques by the appropriate Approved by the global standard.

2.8.1.1.3. Each key component shall provide no knowledge of the key value.

2.8.1.1.4. All materials used in the generation process shall be destroyed after usage In the event of changing a cryptographic key, the new key should be independently generated from the previous key.

2.8.1.2. Key Installation

Key installation is the stage where the key is successfully installed in required each service at the operational site.

2.8.1.2.1. Secret and private keys established using automated methods shall be entered into and output from a cryptographic module in encrypted form.

2.8.1.2.2. Secret and private keys established using manual methods shall be entered into or output from a cryptographic module.

2.8.1.2.3. At least two key components shall be required to reconstruct the original cryptographic key.

2.8.1.3. Key Backup

2.8.1.3.1. The same level of protection as the original cryptographic keys shall be accorded to backup keys.

2.8.1.3.2. When removed from backup storage, all traces of the information in backup storage shall be destroyed.

2.8.1.4. Key Recovery

Key recovery occurs when a key is securely retrieved from Key Backup and re- installed in the Key Installation stage. A key compromise recovery plan must be documented and easily accessible to all relevant parties. The plan must include details of:

2.8.1.4.1. The identity and contact details of the person(s) who should be notified.

- 2.8.1.4.2. The identity and contact details of the person(s) who will perform recovery actions.
- 2.8.1.4.3. An inventory of all keys and their uses shall be maintained.
- 2.8.1.4.4. Steps to identify all information that may be compromised as a result of the incident, and all signatures that may be invalid as a result of the incident.
- 2.8.1.4.5. Method of distribution for new key material and Steps required installing the new key material.

2.8.1.5. Usage of cryptographic keys

The next stage is the Key Usage stage, where the correct key is used for its intended purpose in an operational environment.

- 2.8.1.5.1. Cryptographic keys shall be used for a single purpose to reduce the impact of exposure of a key.
- 2.8.1.5.2. The use of the same key for two different cryptographic processes may weaken the security provided by one or both of the processes and limiting the use of a key will limit the damage or key compromised likelihood.
- 2.8.1.5.3. To reduce the likelihood of improper use, activation and deactivation dates for keys should be defined so that the keys can only be used for the period defined in the associated key management policy.
- 2.8.1.5.4. In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates, which are normally issued by a certification authority, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.
- 2.8.1.5.5. All devices like POS, ATM, or others where Keys and PINs are entered or created must have EPP (Encrypting PIN Pad) with PCI Compliant.
- 2.8.1.5.6. In all transaction logs, whether current or archived must not store PIN Blocks, it should be properly masked.

DOCUMENT CONTROL			
TITLE	Anti-Malware Policy		Effective Date: 11.08.2024
DOCUMENT ID	CRAFT CODE LTD/DOC/POL/0001	Version: 1.0	Page 23 to 27

3. Anti-Malware Policy

3.1. Purpose

CRAFT CODE LTD recognizes the threat of virus as a major risk exposure while carrying on mission-critical functions under a computerized environment and they might be cause them to run erratically, cause loss of information, and information to become corrupted, with the consequential loss of productivity for the organization. Based on the understanding, the CRAFT CODE LTD has designed a separate anti-malware policy.

3.2. Scope

This document sets out the organization's policy about defense against malware and initiate effective precautions by the CRAFT CODE LTD to protect itself against the known and unknown threat events and the topics covered in this document are outlined below;

- External & Internal threat event to inject malware for gain access network, systems of the CRAFT CODE LTD.
- Confidential information disclosed or bot systems.
- Rogue employees within the organization.
- Individuals exercising curiosity or testing their skills.

Compromised CRAFT CODE LTD system by the Malware, the result of a successful security breach where data is compromised is that the CRAFT CODE LTD and its stakeholders are affected. Some areas affected are:

- Network, systems, databases, and applications compromise.
- Financial Damage
- Penalty Fines
- Reputational loss.

Malware-related information and advice for users are included in the associated policy documents referenced below. This control applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties who have access to CRAFT CODE LTD's systems.

The following policies and procedures are relevant to this document:

- Network Security Policy
- Remote Working Policy
- Software Policy
- Information Security Incident Response Procedure
- Configuration Standards for Firewalls, Endpoints, and Servers
- Information Security Policy

3.3. The malware threat

3.3.1. Definition

Malware is any code or software that may be harmful or destructive to the information processing capabilities of the organization. Malicious Software also may be called malicious code or commonly (but inaccurately) "a virus".

3.3.2. Malware Types:

Malware comes in many forms and is constantly changing as previous attack routes are closed and new ones are found. The most common types of malware are:

3.3.2.1. Definitions:

TYPES	DEFINITIONS
Virus	A program that performs an unwanted function on the infected computer. This could involve destructive actions or the collection of information that can be used by the attacker.
Trojan	A program that pretends to be legitimate code but conceals other unwanted functions. Often disguised as a game or useful utility program.
Worm	A program that is capable of copying itself onto other computers or devices without user interaction.
Logic bomb	Malicious code that has been set to run at a specified date and time or when certain conditions are met.
Rootkit	A program is used to disguise malicious activities on a computer by hiding the processes and files from the user
Key logger	Code that records keystrokes entered by the user.
Backdoor	A program that allows unauthorized access at will to an attacker.
Adware	A type of malware that automatically delivers advertisements. Common examples of adware include pop-up ads on websites and those which are displayed by the software.
Bot	An autonomous program that can interact with systems and users for malicious intent
Spyware	A program that enables malicious sources to obtain information about another computer's activity.
Crypto locker /Ransomware	A form of malware that essentially holds a computer system captive while demanding a ransom. Ransomware restricts user access to the computer either by encrypting files on the hard drive or locking down the system. It also displays messages intended to force the user to pay the ransomware creator to remove the restrictions and regain access to their computer.

3.3.3. Malware Spreads Sources (MSS)

For malicious software to carry out its intended purpose, it needs to be installed on the target device or workstations. There are several key ways in which malware infects computers and networks, although new ways are being created all the time. The most common infection techniques are as follows.

3.3.3.1. Phishing

This method involves tricking the user into taking some action that causes a malicious program to run and infect the computer being used. It is usually achieved via the blanket sending of unsolicited emails (Spam) with file attachments or web links included in them. When the user opens the file, or clicks on the link the malicious action is triggered, as protections, CRAFT CODE LTD shall deployed spam controls and awareness training to mitigate such risk.

3.3.3.2. Websites and mobile code

The widespread use of mobile code such as JavaScript on websites has provided attackers with another route to infect computers with malware. Often websites will be created to host the malware which is activated either upon clicking on a link or in some cases simply by visiting the website. Increasingly, legitimate websites are being compromised and made to host malware without the owner's knowledge, making this type of attack very difficult for the user to avoid.

3.3.3.3. Removable media

Access to removable media (USB, CD/DVD) for Desktop/Laptop computers shall be controlled and it's one of the legitimate source to spread out malicious code.

3.3.3.4. Internet

Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people outside of the CRAFT CODE LTD potential access to passwords and other confidential information.

3.3.4. Policy Statement

To prevent the infection of the CRAFT CODE LTD workstation, server, and networks and avoid the potentially dire consequences of such infection, there are several key controls (Intrusions prevention systems, anti-malware protections, threat protections, firewall rule, endpoint security solutions, etc.) that must be adopted as CRAFT CODE LTD environment.

- 3.3.4.1. Firewall

- 3.3.4.1.1. A firewall must be installed at all perimeter areas (MZ, DMZ, Internet Access, etc.) and it might be an internal network, external and partner network of the CRAFT CODE LTD.

- 3.3.4.2. Anti-virus

- 3.3.4.2.1. The Servers and Workstations must be protected from malicious code by ensuring that anti-virus packages are installed, while exceptions (such as Research & Development, Systems used for Security Assessment e.g. Vulnerability Assessment, Penetration Testing, and Forensic, etc.) can be considered upon approval from HOIT.

- 3.3.4.2.2. Users should be aware of the virus alarm and an alarm should be reported to the IT and ADC Ops Division immediately (if any).

- 3.3.4.2.3. Suspected Virus by IT User(s) shall not be deleted/clean unless instructed by the IT and ADC Ops Division.

- 3.3.4.2.4. All anti-virus programs must be configured from a central management console to ensure that the software cannot be disabled or altered by users unless specifically authorized by management on a case-by-case basis for a limited period. This will be quarterly verified by the IT Infrastructure team (Anti-virus Team).

- 3.3.4.2.5. Files received over networks or electronic media shall be scanned for malware/malicious code before use.

- 3.3.4.2.6. 3.3.4.2.6.

- 3.3.4.2.7. Automatic malware scans should be carried out by the Antivirus system on weekly basis.
- 3.3.4.2.8. Attachments to electronic mail must be scanned/checked for malicious code before use.
- 3.3.4.2.9. Users should not double-click on an attachment that contains an executable (EXE, COM, VBS, etc.) that arrives through an e-mail attachment.
- 3.3.4.2.10. An automatic Virus Scan should be in place before downloading any files. Besides, employees shall scan downloaded files from the internet by standard virus prevention software (if any).
- 3.3.4.2.11. Users should not download any unknown or unauthorized application/software which may appear as malicious software from the Internet.

3.3.4.3. Software installation

Users must not have enough administrative access to their workstations to allow them to install software onto it. Only approved software will be allowed, and this must be installed by the IT&ADC Ops department upon authorized request.

3.3.4.4. Malware incident management

If malware is detected on a server, client, network, or other IT component, an information security incident must be raised. This will be managed by the procedures set out in the Information Security Incident Response Procedure.

3.3.4.5. Threat monitoring and alerts

Information about emerging threats must be obtained from appropriate sources and users alerted proactively of potential attacks, giving as much detail as possible to maximize the chance of recognition. Intrusion prevention systems (IPS) must be deployed on all networks to monitor traffic for malicious activity or policy violations. Any detected activity or violation will be reported either to an administrator or collected Centrally using a security information and event management (SIEM) system and reported to the management regarding severity level.

3.3.5. Configuration standard

A configuration standard is a pre-defined and approved list of settings/configurations and software/hardware installations per device (firewall, endpoint, servers, etc.). Part of a configuration standard includes the concept of 'system hardening' which is designed to lower the attack surface and risk of a cyber-attack. All devices will be deployed using a configuration standard. Further information can be found in the Network Security Policy

3.3.6. Technical Reviews

Regular reviews will be carried out of business-critical servers and networks to identify any malware that has been installed since the last review. This will include the taking of a snapshot of the configuration for later comparison purposes and reported to the ICT security team.

DOCUMENT CONTROL			
TITLE	Access Control Policy		Effective Date: 11.08.2024
DOCUMENT ID	CRAFT CODE LTD/DOC/POL/0004	Version: 1.0	Page 28 to 32

4. Access Control Policy

4.1. Purpose

The control of access to the information assets is a fundamental part of the defense-in-depth approach to information security. To effectively protect the confidentiality, integrity, availability, and non-repudiation of classified data, the CRAFT CODE LTD shall be followed a comprehensive mixed model of physical and logical controls are in place.

4.2. Scope

The purpose of the policy is to ensure the appropriate control mechanism to reduce fraudulent activities as well as protected business objectives and goals. Therefore, this policy must be based upon a clear understanding of the business requirements as specified by the owners of the assets involved. These requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service.
- Relevant legislation that may apply e.g. Bangladesh CRAFT CODE LTD guideline, PCI DSS, etc.
- The regulatory framework.
- Contractual obligations to external third parties.
- The threats, vulnerabilities, and risks involved
- The organization's appetite for risk.
- Accountability and non-repudiation ensure.

This access control policy is designed to take account of the business and information security requirements of the organization and is subject to regular review to ensure that it remains appropriate. This control applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties who have access to CRAFT CODE LTD's systems. The following policies and procedures are relevant to this document and referred policy maintains separate by the CRAFT CODE LTD Ltd:

- Mobile Device Policy
- Remote Working Policy
- Network Security Policy
- Internet Acceptable Use Policy
- Information Security Policy

4.3. Policy Statement:

A formal user access control policy must be documented, implemented, and kept up to date for each application and information system to ensure only authorized user access and to prevent unauthorized access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated and system administration accounts maintain to perform system administration tasks and all activities routed through Privilege access management systems.

- 4.3.1. User Registration and Deregistration

- 4.3.1.1. A request for access to the organization's network and workstations, applications, email, and others business requirements systems, the user must be submitted requisitions with competent approval authority.
- 4.3.1.2. User requests will be processed according to the CRAFT CODE LTD procedure, which ensures appropriate security checks are carried out and correct authorization is obtained before user account creation.
- 4.3.1.3. The principle of segregation of duties will apply so that the creation of the user account and the assignment of permissions are performed by the different people.
- 4.3.1.4. Each user account will have a unique username that is not shared with any other user and is associated with a specific individual i.e., not a role or job title.
- 4.3.1.5. Generic user accounts i.e. single accounts to be used by a group of people must not be created as they provide an insufficient allocation of responsibility.
- 4.3.1.6. An initial strong password must be created on account setup and communicated to the user via secure means. The user must be required to change the password on the first use of the account.
- 4.3.1.7. When an employee leaves the organization under normal circumstances, their access to workstations systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the IT & ADC Ops Department.
- 4.3.1.8. In exceptional circumstances where there is perceived to be a risk that the employee may take action that may harm the organization before or upon termination, a request to remove access may be approved by the HRD or competent authority, and actioned in advance of notice of termination is given. This precaution will especially apply in the case where the individual concerned has privileged access rights e.g. domain admin, Network manager, software Developer, database, and applications owners.
- 4.3.1.9. User accounts must be initially suspended or disabled only and not deleted. User account names must not be reused as this may confuse the event of a later investigation.

- 4.3.2. User access provisioning

- 4.3.2.1. Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform. In general, this will be role-based i.e. a user account will be added to a group that has been created with the access permissions required by that job role.
- 4.3.2.2. Group roles must be maintained in line with business requirements and any changes to them must be formally authorized and controlled via the change management process.
- 4.3.2.3. Ad-hoc additional permissions must not be granted to user accounts outside of the group role, if such permissions are required, this must be addressed as a change and formally requested.

- 4.3.3. Access to customer networks and systems

- Access is often needed to customer's networks and systems to provide services and support. Unique user accounts and unique strong (Complex) passwords (CRAFT CODE LTD Password Policy) will be used for each customer.

- 4.3.4. Review of user access rights

- 4.3.4.1. Regularly (at Quarterly/Half-yearly and yearly) asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place. This will be to identify:
 - People who should not have access (e.g. leavers)
 - User accounts with more access than required by the role.
 - User accounts with incorrect role allocations.
 - User accounts that do not provide adequate identification e.g. generic or shared accounts.
 - Any other issues that do not comply with this policy.
- 4.3.4.2. This review will be performed according to a formal procedure and any corrective actions identified and carried out.
- 4.3.4.3. A review of user accounts with privileged access will be carried out by the IT Security Manager quarterly to ensure that this policy is being complied.

- 4.3.5. System and application access control

- As part of the evaluation process for new or significantly changed systems, requirements for effective access control must be addressed and appropriate measures implemented. These will consist of a comprehensive security model that includes support for the following:
 - 4.3.5.1. Creation of individual identical user accounts.
 - 4.3.5.2. Definition of roles or groups to which user accounts can be assigned.
 - 4.3.5.3. Allocation of permissions to objects (e.g. files, programs, menus) of different types (e.g. read, write, delete, execute) to subjects (user accounts and groups)

- 4.3.5.4. Provision of varying views of menu options and data according to the user account and its permission levels.
- 4.3.5.5. User account administration, including the ability to disable and delete accounts
- 4.3.5.6. User logon controls such as:
 - Non-display of the password while entered.
 - Account lockout once several incorrect logon attempts exceed more than three (3) times.
 - Provide information about the number of unsuccessful login attempts and the last successful login once.
 - Date and time-based login restrictions were maintained.
 - Device and location logon restrictions.
- 4.3.5.7. User inactivity session timeout shall be maintained.
- 4.3.5.8. Password management, including
 - The ability for the user to change the password.
 - Controls over acceptable passwords.
 - Password expiry and history controls are maintained.
 - Hashed/encrypted password storage and transmission.
- 4.3.5.9. Security auditing facilities, including logon/logoffs, unsuccessful logon attempts, object access, and account administration activities must be recorded.
- 4.3.5.10. Default 'deny all' access to systems and system components unless specifically allowed.
- 4.3.5.11. Where modified software development is undertaken, program source code must be protected from unauthorized access.
- 4.3.5.12. Access to utility programs that provide a method of bypassing system security (e.g. data manipulation tools) must be strictly controlled and their use restricted to identified individuals and specific circumstances e.g. as part of a named project or change.
- 4.3.5.13. 4.3.5.13.

DOCUMENT CONTROL			
TITLE	Password Policy		Effective Date: 11.08.2024
DOCUMENT ID	CRAFT CODE LTD/DOC/POL/0005	Version: 1.0	Page 33 to 36

5. Password Policy

5.1. Purpose:

Passwords are considered as the primary method to ensure there is no unauthorized access to CRAFT CODE LTD's networks and systems. The threat posed by unauthorized access can be very serious and can have costly implications to the organization and its stakeholders. Therefore, it is important to ensure there is a well- considered password policy documented, in use and known to all staff, vendors and third parties who have access to the organization's IT systems and data.

5.2. Scope:

The effectiveness of a password is largely determined by the design and implementation of the authentication system, how frequently password attempts can be made by an unauthorized user and the security methods used to protect users' passwords at the point of entry, during transmission, and while in storage.

Authentication requires one of the following:

- Something you know, such as a password or passphrase
- Something you have, such as a token device/app or smart card
- Something you are, such as biometric (e.g. finger print readers)

It is the responsibility of all employees, stakeholders, vendors and third-party suppliers to comply with this policy. The IT department is responsible for enforcing the password policy where technically possible. Frequent reviews of all IT systems are undertaken to ensure the effectiveness of password authentication.

5.3. Policy Statement

Passwords are an important aspect of computer security and the front line of protection for user accounts. A poorly chosen password may result in a compromise of CRAFT CODE LTD's entire network. As such, users are responsible for taking the appropriate steps, as outlined below, to select and secure password. The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of passwords, and the frequency of change.

- 5.3.1. Default passwords should not be used (i.e. all vendor-defined default passwords must be changed, disabled, or locked before the system is used).
- 5.3.2. All password entries must be masked.
- 5.3.3. Local administrator password on user PC(s)/server(s)/equipment(s) will not provide to end- users. Only authorized and respective IT persons will hold the credentials.
- 5.3.4. Administrative passwords of the Operating System, Database, and Business Applications shall be kept in safe custody with a sealed envelope.
- 5.3.5. All user-level passwords (e.g., email, web, desktop computer, etc.) must follow the following guidelines.

Minimum Password Length	8 (Alphanumeric)
Enforce Mixed Case	Yes
Enforce Numerals	Yes
Enforce Special Characters	Yes
Enforce Starting with an Alphabet	Yes
The account will lock the unsuccessful login attempt	3
Password can contain login Name	No
Reuse of old Passwords (Password History)	Don't allow last 3 Passwords
Maximum Password Age	90 days

- 5.3.6. All system-level passwords (e.g., root, enable, sys, network administrator, application administration accounts, application connection account, etc.) must follow the below guidelines.

Minimum Password Length	8 (alphanumeric)
Enforce Mixed Case	Yes
Enforce Numerals	Yes
Enforce Special Characters	Yes
Enforce Starting with an Alphabet	Yes
Password can contain login Name	No
Reuse of old Passwords (Password History)	Don't allow last 3 Passwords
Maximum Password Age	180 days

- 5.3.7. CRAFT CODE LTD encourages using a password length of more than 8 characters.
- 5.3.8. The account that is no longer needed must be deleted/disabled/lock.
- 5.3.9. Any employee found to have violated this password policy may be subject to disciplinary action, up to and including termination of employment.
- 5.3.10. If an account or password is suspected to have been compromised, report the incident to HOD/line manager and IT and ADC Operations Division and change respective passwords immediately.
- 5.3.11. Password cracking or guessing may be performed on a periodic or random basis by the IT and ADC Operations Division. If a password is guessed or cracked during one of these scans, the responsible user will be required to change the password upon intimation by the IT and ADC Operations Division.
- 5.3.12. All passwords are to be treated as sensitive, Confidential CRAFT CODE LTD's information. Here is a list of "do not's".
 - Don't reveal a password over the phone to anyone
 - Don't talk about a password in front of others
 - Don't hint at the format of a password (e.g., "my family name")
 - Don't reveal a password on questionnaires or security forms
 - Don't share a password with family members
 - Don't reveal a password to a co-worker while on vacation
 - Don't use the "Remember Password" feature of applications
 - Don't store passwords in a file on ANY computer system unencrypted.
 - Don't write down password anywhere
 - Don't auto-complete/Password storage option in-brows

5.4. Guideline for password policy

5.4.1. General

The following rules are based on guidance from Bangladesh CRAFT CODE LTD guideline, UK NCSC (National Cyber Security Centre) and the USA National Institute of Standards and Technology (NIST). Where possible, passwords will have the following characteristics:

- 5.4.1.1. Password expiry will be used.
- 5.4.1.2. Password complexity requirements will not be used (e.g. specifying that a password must contain special characters and numbers)
- 5.4.1.3. Single Sign-On (SSO – where a user is authenticated once and then has access to many systems) will be used where available and appropriate.
- 5.4.1.4. Throttling techniques (where an increasing time delay is introduced between logon attempts) will be used where available.
- 5.4.1.5. After three unsuccessful login attempts are made, the user account will be locked out and will need to be re-enabled by an administrator.
- 5.4.1.6. A password blacklist will be utilized to prevent the use of common, easily-guessed passwords.
- 5.4.1.7. If a session has been idled for a period of 15 minutes, the user will be required to re-authenticate.
- 5.4.1.8. Newly-issued passwords will be subject to change immediately after first use.
- 5.4.1.9. System default accounts/passwords will be disabled/changed immediately as part of initial setup and configuration.

DOCUMENT CONTROL			
TITLE	Physical Security Policy		Effective Date: 11.08.2024
DOCUMENT ID	CRAFT CODE LTD/DOC/POL/0006	Version: 1.0	Page 37 to 39

6. Physical Security Policy

6.1. Purpose:

The protection of the physical environment is one of the most obvious yet most important tasks within the area of information security. A lack of physical access control can undo the most careful technical precautions and potentially put lives at risk.

Craft Code Ltd. is committed to ensuring the safety of its employees, contractors, and assets, etc. take the issue of physical security very seriously. This policy sets out the main precautions that must be taken.

6.2. Scope:

This control applies to all offices, systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties who have access to the CRAFT CODE LTD's resources.

6.3. Secure areas

Sensitive information must be stored securely. A risk assessment must be carried out to identify the appropriate level of protection to be implemented to secure the information being stored. Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted.

- 6.3.1. A building must have appropriate control mechanisms in place for the classification of information and equipment that is stored within it.

These may include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours.
 - Window and door locks.
 - Window bars on lower floor levels.
 - Access control mechanisms fitted to all accessible doors (where codes are utilized they should be regularly changed and known only to those people authorized to access the area/building).
 - CCTV cameras (recordings kept for at least 3 months data).
 - Staffed at the reception area.
 - Protection against damage - e.g. fire, flood, vandalism.
- 6.3.2. Staff working in secure areas must challenge anyone not wearing a badge.
 - 6.3.3. Identification and access tools/passes (e.g. badges, keys, entry codes, etc.) must only be held by persons authorized to access those areas and must not be allowed/provided to anyone else.
 - 6.3.4. Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge.
 - 6.3.5. An organization employee must always monitor all visitors accessing secure areas.
 - 6.3.6. Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by the IT function as appropriate.
 - 6.3.7. Where breaches do occur, or an employee leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys, etc.) must be recovered from the employee and any door/access codes changed immediately.
 - 6.3.8. Offsite backup locations will be reviewed at least annually to ensure these locations are physically secure for the media backups.

6.4. Paper security

Paper in an open office must be protected by the controls for the building and via appropriate measures that may include, but are not restricted to, the following:

- 6.4.1. Filing cabinets that are locked with the keys stored away from the cabinet.
- 6.4.2. Locked safes.
- 6.4.3. Stored in a secure area protected by access controls.
- 6.4.4. Paper deposable containers secured.

6.5. Equipment Security

All general computer equipment must be in suitable physical locations that:

- 6.5.1. Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust, and vibration.
- 6.5.2. Limit the risk of theft – e.g. if necessary, items such as laptops should be physically attached to the desk.
- 6.5.3. Allow workstations handling sensitive data to be positioned to eliminate the risk of the data being seen by unauthorized people.
- 6.5.4. Restrict physical access to wireless access points and gateways devices.
- 6.5.5. Data will be stored on network file servers where appropriate. This ensures that information lost, stolen, or damaged via unauthorized access can be restored and its integrity maintained.
- 6.5.6. All servers located outside of the data center must be sited in a physically secure environment.
- 6.5.7. Business-critical systems must be protected by an Uninterruptible Power Supply (UPS) to reduce the operating system and data corruption risk from power failures.
- 6.5.8. All items of equipment must be recorded, both on the departmental and the overall CRAFT CODE LTD inventory. Procedures must be in place to ensure inventories are updated as soon as assets are received or disposed of.
- 6.5.9. All equipment must be security marked and have a unique asset number allocated to it. This asset number will be recorded in the departmental and the overall CRAFT CODE LTD inventories.
- 6.5.10. Cables that carry data or support key information services must be protected from interception or damage.
- 6.5.11. Power cables must be separated from network cables to prevent interference. Network cables must be protected by conduit and where possible avoid routes through public areas.
- 6.5.12. Physical and/or logical controls must be implemented to restrict access to publicly accessible network ports on office walls, for example, network ports located in public areas and areas accessible to visitors will be disabled and only enabled when network access is explicitly authorized.
- 6.5.13. Device tamper inspections will be performed and recorded to ensure payment devices are not compromised. Training will be provided to staff members to inspect devices appropriately.

DOCUMENT CONTROL			
TITLE	Internet Acceptable Use Policy	Effective Date: 11.08.2024	
DOCUMENT ID	CRAFT CODE LTD/DOC/POL/0007	Version: 1.0	Page 40 to 43

7. Internet Acceptable Use Policy

7.1. Introduction:

Internet use brings the possibility of breaches of the security of confidential company information. Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people outside of the Craft Code Ltd potential access to passwords and other confidential information. Despite considering the risk factor to access the internet of an employee of Craft Code Ltd is permitted and encouraged where such use supports the goals and objectives of the business.

7.2. Purpose:

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at Craft Code Ltd in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

Craft Code Ltd provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

7.3. Objective and Scope:

This policy covers all internet facilities that are provided by Craft Code Ltd to conduct and support official business activity through the organization's network infrastructure and all mobile devices. All employees of the Craft Code Ltd (Permanent, contractual or temporary staff) who have been gained the right to use computer devices, networks, and other electronic information systems are required to sign this agreement confirming their understanding and acceptance of this policy.

The objective of this policy is to direct all users of the Internet by:

- 7.3.1. Guiding expected working practice.
- 7.3.2. Highlighting issues affecting the use.
- 7.3.3. Describing the standards that users must maintain
- 7.3.4. Stating the actions that may be taken to monitor the effectiveness of this policy
- 7.3.5. Warning users about the consequences of inappropriate use of the Internet service

7.4. Policy Statement:

Considering the internet uses risk in the CRAFT CODE LTD environment, below are the policy statement detail whereby must obey as well as ensure that they:

- 7.4.1. Separate approval requests are required to avail of Internet access. The request should be approved by the HOD/line manager from the concerned department. However, considering sensitivity and security, HOIT may approve/reject the access request upon discussion with the line manager.

- 7.4.2. The employee shall be awarded security consciousness about the use of the Internet.
- 7.4.3. Access to the Internet from CRAFT CODE LTD premises and systems must be routed through secure gateways (e.g. firewall, Router device along with restricted controls).
- 7.4.4. Any local or separate internet connection at the CRAFT CODE LTD premises or systems, including standalone PCs and laptops, is prohibited unless allowed by the competent authority of the IT & ADC Operation Division.
- 7.4.5. Employees shall be prohibited from establishing their network connection to the Internet using CRAFT CODE LTD workstations, systems, or premises.
- 7.4.6. The use of locally attached modems with CRAFT CODE LTD's systems to establish a connection with the Internet or any third-party or public network via broadband, ISDN, or PSTN services are prohibited unless specifically approved.
- 7.4.7. The provided Internet access by the CRAFT CODE LTD must not be used to conduct an own commercial business/activity that is not done by the CRAFT CODE LTD.
- 7.4.8. Internet access provided by the CRAFT CODE LTD must not be used to engage in any activity that knowingly contravenes any criminal or civil law or act. Any such activity will result in disciplinary action of the personnel involved.
- 7.4.9. All applications and systems that require connections to the Internet or third-party and public networks must undergo a formal risk analysis during development and before production use and all required security mechanisms must be implemented.
- 7.4.10. The employee must be security concerned about the use of the Internet.
- 7.4.11. Unnecessary or unauthorized Internet usage must be avoided.
- 7.4.12. Users should not do anything (e.g. large file share) that causes network congestion.

7.5. Internet Acceptable Use Policy:

- 7.5.1. Business use of the internet service

The internet access must be used following this policy for tasks reasonably related to work including:

- 7.5.1.1. Access to information that is relevant to fulfilling the organization's business obligations.
- 7.5.1.2. The internet user maintains access for relevant business purposes, not personal purposes.

7.5.2. Personal use of the Internet service

- 7.5.2.1. If any employee purchases personal goods or services via the Internet service, he/she is responsible for ensuring that the information you provide shows that the transaction is being entered into by self and not on behalf of CRAFT CODE LTD.
- 7.5.2.2. User shall ensure that personal goods and services purchased are delivered to home or other personal address and not delivered to organization property.
- 7.5.2.3. If an employee is in any doubt about how he/she may make personal use of the Internet Service, he/she is advised not to do so.

- 7.5.2.4. User's workstation and company-provided mobile devices and any data held on them are the property of CRAFT CODE LTD and may be accessed at any time by Craft Code Ltd to ensure compliance with all its statutory, regulatory, and internal policy requirements.

7.6. Prohibited Uses of the internet service

Internet user shall be followed strictly and necessarily required for work and must not use Internet account to below purpose/Prohibited statement:

- 7.6.1. Create, download, upload, display, or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene, or offensive.
- 7.6.2. Subscribe to, enter, or use peer-to-peer networks or install software that allows sharing of music, video, or image files
- 7.6.3. Subscribe to, enter, or utilize real-time chat facilities such as chat rooms, text messenger, or pager programs
- 7.6.4. Subscribe to, enter, or use online gaming or betting sites
- 7.6.5. Subscribe to or enter "money-making" sites or enter or use "money-making" programs.
- 7.6.6. Run a private business.
- 7.6.7. Download any software that does not comply with the organization's software policy
- 7.6.8. The above list gives examples of "unsuitable" usage but is neither exclusive nor exhaustive. "Unsuitable" material would include data, images, audio files, or video files the transmission of which is illegal and material that is against the rule, essence, and spirit of this and other organizational policies.
- 7.6.9. The organization will take steps to block the following categories of websites: Illegal, Pornographic, Violence, Hate and discrimination, Offensive, Weapons, Hacking, Webchat, Gambling, Dating, and Radio stations, Games, Streaming Media.
- 7.6.10. If any user has inadvertently attempted to access such as the site you should inform the IT department immediately through Service request or mail.

DOCUMENT CONTROL			
TITLE	Employee Screening Policy	Effective Date: 11.08.2024	
DOCUMENT ID	CRAFT CODE LTD\DOC\POL\0008	Version: 1.0	Page 44 to 45

8. Employee Screening Policy

8.1.Purpose:

The purpose of this Policy is to ensure adequate checks are established to determine and/or confirm, within appropriate legal and professional limits, the qualifications and suitability of a job candidate for roles within the Organization.

8.2. Scope:

The employee screening policy or Personnel Security Policy applies to all applicants and employees; full-time and part-time. All personnel (such as employees, agents, consultants, and contractors) with operational (maintenance or administration) access to the CRAFT CODE LTD's systems and shall check below controls before employment;

Background checks may include:

- Criminal records & details of any past or pending civil or criminal proceedings.
- Credit reports.
- Identity Verification reports.
- Reference checks - Previous employment, Education certificate verifications.
- Sex & Violent Offender Registry Check
- Reference verifications according to CV references
- Validation of any involvement in external businesses that could result in a conflict of interest.
- Depending on the nature of the work being performed, additional components could include: Pre-employment Physical (Facilities).
- Physical and Mental fitness may be medical tests / interviewed.

8.3. Policy Statement

- 8.3.1. Background checks are required prior to employing employees, regardless of if a competitive recruitment process is used.
- 8.3.2. Background checks may be required for employees who change positions in the District, obtaining more sensitive duties, as determined by Human Resources or the hiring manager.
- 8.3.3. Background checks may be required for employees at any time after the employment start date, at the discretion of Human Resources or Executive Management.

8.4. Reference Check Process

- 8.4.1. Educational Record Check A new joiner must submit copies of all academic certificates along with the originals to HRD. Original Certificates will be returned after verification. If any doubt, genuineness of certificate to be verified from issuers.
- 8.4.2. Medical Fitness Examination All employees will be required to undergo a physical fitness test to be undertaken by Management approved medical centers in accordance with requirements to be defined by HRD. Executive Medical test to be done. Test report to be maintained in personal file.
- 8.4.3. Others verifications Verifications should take into account all relevant privacy, protections of personally identifiable information and employment based legislation and should, where permitted, including following;
 - Availability of satisfactory clearance references from previous organizations or one personal.
 - Verifications (for completeness and accuracy) of the applicant's curriculum vitae.

- Confirmations of claimed academic and professional qualifications.
- Independent identity verifications (passport or similar document like National ID Card)
- Detail verifications such as credit review (like CIB) or review of criminal records like policy verifications.
- For fresher reference letters from two respectable persons of the society acceptable to the LTD.

Data Protection Policy

Craft Code Ltd.

Policy Creation Date	14.08.2024
----------------------	------------

1. Data protection principles

Craft Code Ltd is committed to processing data in accordance with its responsibilities under the Digital Security Act,2018.

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and Ltd to what is necessary for relation to the purposes for which they are processed;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. General provisions

- This policy applies to all personal data processed by Craft Code Ltd.
- The Responsible Person shall take responsibility for Craft Code Ltd's ongoing compliance with this policy.
- This policy shall be reviewed at least annually.
- Craft Code Ltd is certified with "PCI DSS" from "Right Time Ltd"

3. Lawful, fair and transparent processing

- To ensure its processing of data is lawful, fair and transparent, Craft Code Ltd shall maintain a Register of Systems.
- The Register of Systems shall be reviewed at least annually.

4. Lawful purposes

- a. All data processed by Craft Code Ltd must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
- b. Craft Code Ltd shall note the appropriate lawful basis in the Register of Systems.
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt- in consent shall be kept with the personal data.

5. Data minimization

- a. Craft Code Ltd shall ensure that personal data are adequate, relevant and Ltd to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

- a. Craft Code Ltd shall take reasonable steps to ensure personal data is accurate.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

- a. To ensure that personal data is kept for no longer than necessary, Craft Code Ltd shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

- a. Craft Code Ltd shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- b. Access to personal data shall be Ltd to personnel who need access and appropriate security should be in place to avoid unauthorized sharing of information.
- c. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, Craft Code Ltd shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach accordingly.

END OF POLICY

Document Title /Name	Password Management Standard
Current Version	4.0
Document/Policy Owner	Chief Operating Officer
Document Author	Tasnim Hosen
Approver	Colin Patra, Managing Director
Effective From	17 November 2024
Next Revision Date	15 December 2025
Document Type/Classification	Internal
Document Font	Times New Roman
File Name	Password Management Standard_v4.0

Certificate of Approval
“Password Management Standard”

Has Been Approved By
Colin Patra
Managing Director

Reviewed By
Tasnim Hossain
Chief Operating Officer

Contact Department:

In the event of queries, or request for copies, please contact:

CRAFTCODE LTD

2. INTRODUCTION

Passwords are an important aspect of system/ network security. They are the front line of protection ensuring logical access controls on applications, devices, security devices, laptops and desktops. As such, all Craft Code Ltd. (hereafter referred as Craft Code) users (including contractors and third party employees having access to Craft Code's information systems) are responsible for taking the appropriate precautions/steps, as outlined below, to select and secure their passwords. The purpose of this document is to provide a set of minimum security standards to be implemented on Craft Code's IT systems and network components for password management.

2. SCOPE

The Password Management Standard is applicable to web servers, database servers, application servers, file servers, mail servers, name servers, FTP servers, in-house developed/ outsourced applications, laptops/ desktops, network devices and security infrastructure devices such as firewalls and IPS/ IDS and other devices with login capability within Craft Code.

All new systems should be compliant to this standard before commissioning and system commissioned before the effective date of this standard shall be made compliant as per technical feasibility.

3. RESPONSIBILITY

Respective asset/service owners are responsible to implement this standard for any new systems/nodes and respective asset custodians are responsible for enforcing & maintaining all applicable passwords and account controls on all systems that process, store or transmit any Craft Code information.

GM, technical compliance is responsible for ensuring that all administrators are aware of this standard. This may include, but is not limited to:

- Providing access to a copy of the Standard, for example, on the intranet,
- Reminders of the need for compliance with the Standard, and
- Providing updates or developments of the Standard.

It is the responsibility of all Craft Code employees to abide by this standard.

4. PASSWORD & ACCOUNT CONTROLS

A summary of suggestive mandatory password controls and optional password controls based on asset criticality / User type is provided in Section 6. Wherever possible, all password controls mentioned below should be enforced by Craft Code.

4.1. Strong Password Controls

4.1.1. Password Length

- Minimum password length shall be 10

4.1.2. Password Complexity Requirements

- Passwords should contain at least three out of these four: One numbers, one capital alphabet. One small alphabet, One Special character (E.g.: !, ?, #, %, *)

4.1.3. Password Age

- Maximum Password age/expiry period shall be between 45 to 60 days
- Minimum password age shall be 1 day unless the password is a reset by administrator or initial password
- Minimum Password age is not applicable for specific on boarded user account managed by administrator

4.1.4. Password History

- Users shall not re-use at-least the last 5 passwords

4.2. Other Password Controls

- 4.2.1. Default Password

- All system/application default passwords, including service accounts, must be changed before the system is migrated to the production environment. This shall be ensured by the respective system administrator before go-live.

- 4.2.2. Initial Password

- Systems must assign a unique initial password to every user account, which the user should be forced to change upon subsequent login.

- 4.2.3. Password Storag

- Password should not be stored in plain text format in any purpose.
- Passwords should be stored in encrypted format using irreversible encryption algorithms like SHA-256, SHA-512, MD5, salted MD5 etc.
- This shall be embedded in the system design.

- 4.2.4. Prohibited Password

- Passwords should not contain the user's account name. Passwords should not have keyword "Craft Code"

4.3. Account Password Controls

- 4.3.1. Account Lockout Threshold

- Except for super-administrator accounts, the number of allowed unsuccessful log-on attempts is up to 5 (Five) attempts.

- 4.3.2. Account Lockout Duration

- A time delay of minimum 15 minutes shall be forced before further log-on attempts are allowed

- 4.3.3. Account Session Time Out Duration

- System/Applications should have a maximum of 120 minutes as idle session time-out, except for integration users

5. PASSWORD CONTROL MATRIX

- 5.1. Strong Password Matrix

- The following Automated/ System level controls provides a suggestive list of password parameters that need to be complied to:

Clause	Password Parameters	Other users		Integration Users
		Critical Systems	Other Systems	
4.1.1	Password Length	Mandatory	Mandatory	Mandatory
4.1.2	Password Complexity	Mandatory	Mandatory	Mandatory
4.1.3	Password Age	Mandatory	Optional if number of users are less than 25	Optional
4.1.4	Password History	Mandatory	Optional if number of users are less than 25	Optional

Notes: ^^All expired passwords shall be changed at least once a year.

- 5.2. Other default controls

- The following provide a suggestive list of password controls that need to be complied:

Clause	Password Parameters	Other users		Integration Users
		Critical Systems	Other Systems	
4.2.1	Remove default password	Mandatory	Mandatory	Mandatory
4.2.2	Initial Password	Mandatory	Optional if number of users are less than 25	Optional
4.2.3	Prohibited Password	Mandatory	Mandatory	Mandatory
4.2.4	Secure Password Storage	Mandatory	Mandatory	Mandatory

- 5.3. Account controls

- The following Automated/ System level controls provides a suggestive list of password parameters that need to be complied for Account Passwords:

Clause	Password Parameters	Other users		Integration Users
		Critical Systems	Other Systems	
4.3.1	Account Lockout threshold set to 5 unsuccessful log on attempts	Mandatory	Optional if number of users are less than 25	Optional
4.3.2	Account Lockout duration	Optional (Mandatory for AD)	Optional	Optional
4.3.3	Account Session timeout duration	Mandatory	Optional if number of users are less than 25	Optional

6. Controls applicability

All password controls (except clause 4.2.1, 4.2.3 and 4.2.4) mentioned should be automatically enforced by the system. However, if it is not possible to enforce the password controls automatically by the system due to commercial/technical limitations and has less than 10 users (per IP/interface), manual password controls could be implemented by the respective users wherein automated controls are optional.

7. One time Password (OTP)

- 7.1. OTP Length: length minimum 6
- 7.2. Password Complexity requirements: Complexity optional
- 7.3. Password Age: Minimum Age 0 maximum age 5 min (preferred 60 sec)
- 7.4. Account controls points will also be applicable for OTP

Notes: OTP PIN minimum length 4, complexity optional and max age 6 month if multi factor (PIN+OTP/password etc) used.

8. Key Based Authentication

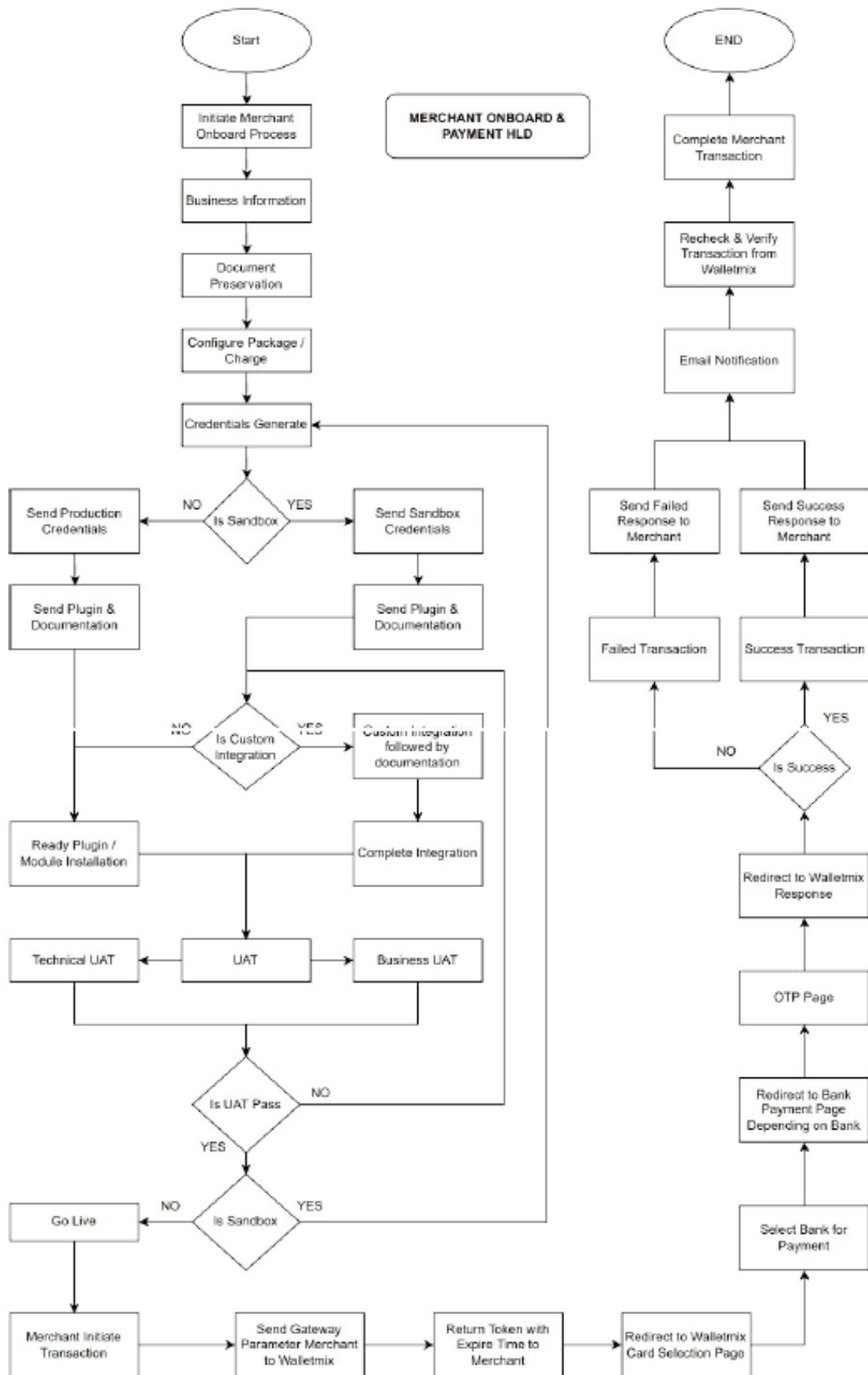
- 8.1. Key based authentication can be used as an additional mechanism to password controls
- 8.2. Unique Key must be generated for individual authentication
- 8.3. Recommended lengths is 4096 bits

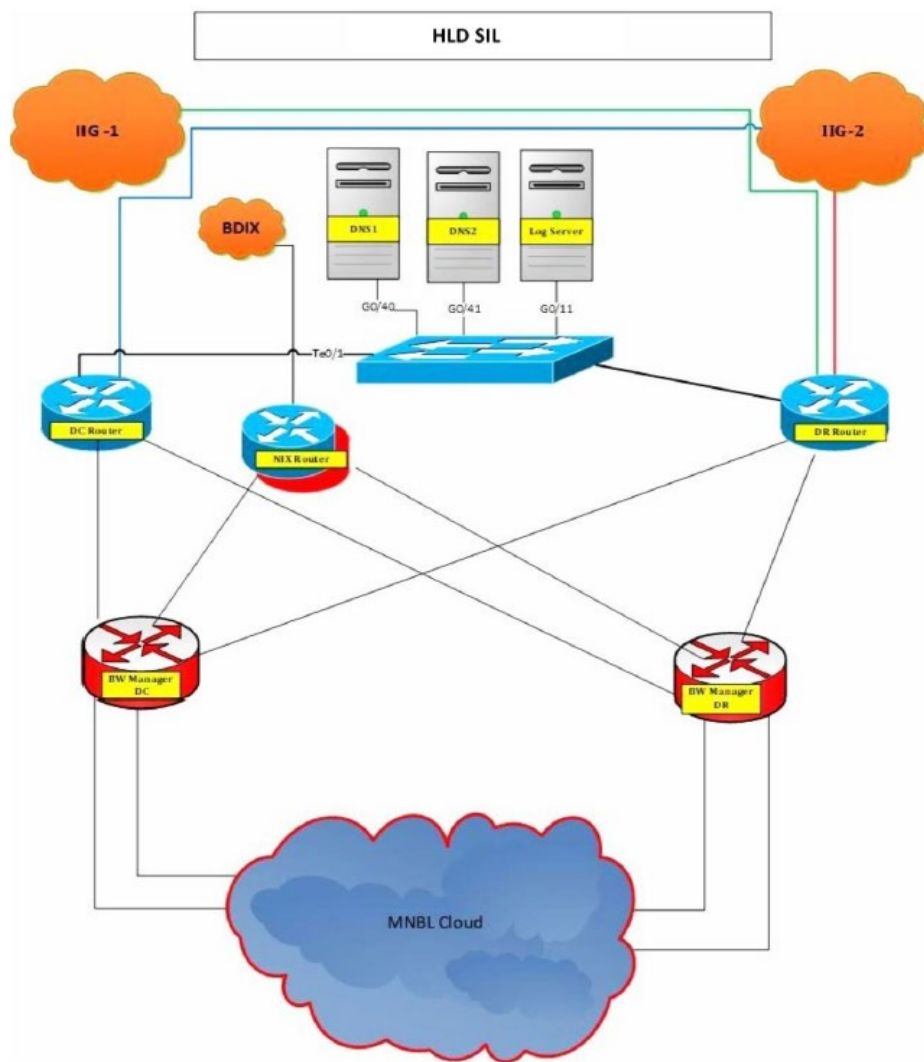
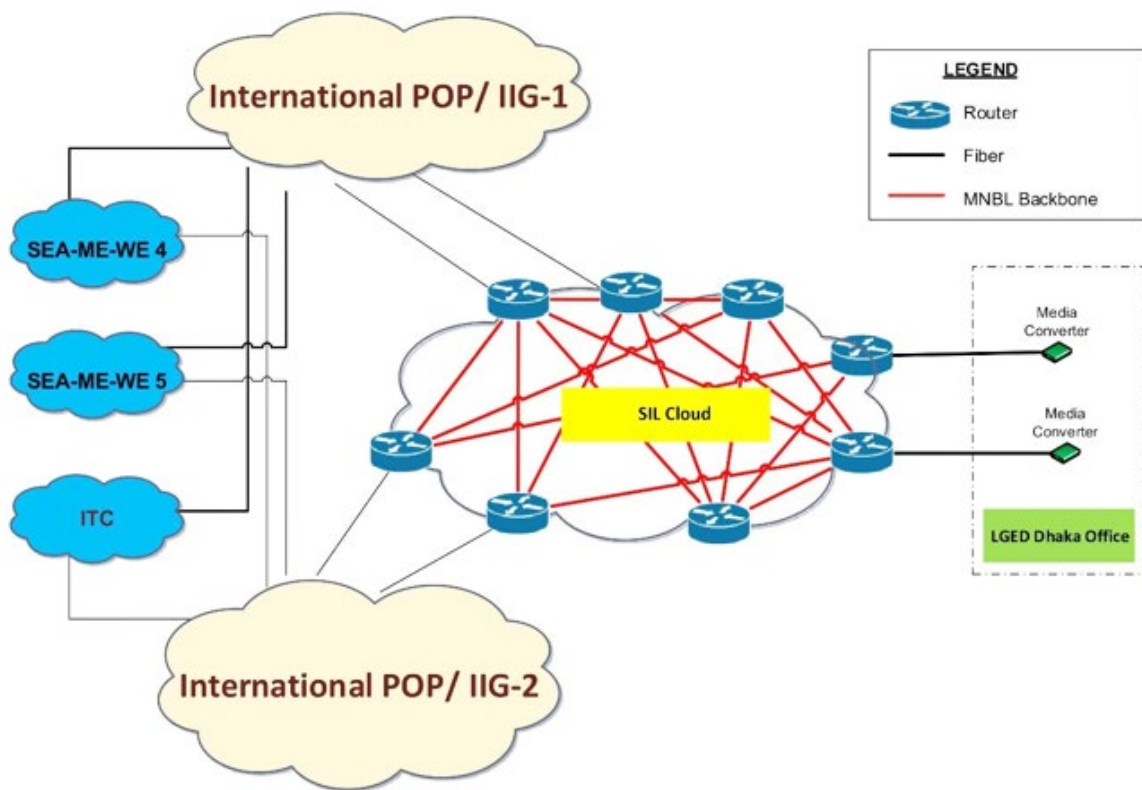
9. EXCEPTION

If any control has implementation discrepancies, then the same must be recorded by the system owners/custodians, justified with risk assessment where applicable endorsed by CTO and CIO approved by the CXOs. Any risk to be listed in the risk register should be aligned with Compliance team.

10. ENFORCEMENT

All department head of IT & Technology will be responsible to enforce this Standard at their level.





Functional Requirement Specification (FRS)

Project Name: Payment Gateway powered by Craft Code Ltd.

Company Name: Craft Code Ltd.

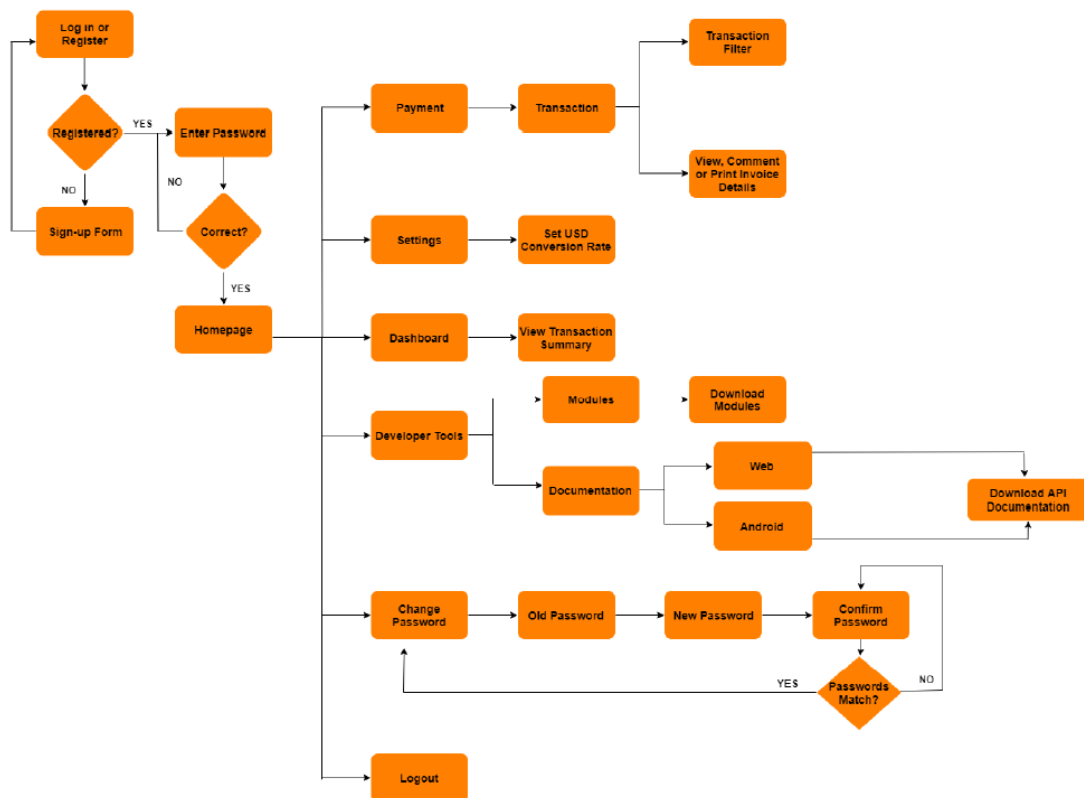
Change History Record

Sl.	Date	Version	Description	Changed by	Approved by
1	08/10/2024	1.00	Initial Version	Tasnim	Tasnim Hosen

1. Introduction

Any business that does not provide online payment solutions is missing out on a huge chunk of business revenue not to mention potential customer base. Our Payment gateway allows you to merchandise your products or services online and automatically process credit cards, debit cards or other forms of payment. This payment gateway service includes security measures that verify each credit card number and intercept potential criminal attempts before a transaction takes place. It has everything from merchant accounts to customized web stores. This payment gateway is ideal for customers with online wallets. It provides a handful of credit card processing solutions ideal for web and traditional business models.

2. Software Architecture Diagram powered by Craft Code Ltd.



3. Functional Requirement

The functions of this application are categorized into different USE CASES in this section. Please check the following use cases to understand and define the functionality of this application Payment Gateway.

- 3.1MERCHANT (ADMIN SIDE)

- 3.1.1 New Merchant

New Merchant

Scope ID	G.1.1
General Description	This section will describe the basic information about the Create Merchant Account

- 3.1.2 Attribute List

Attribute Name	Description	Effect/Impact
User Name	<i>Need to enter manually</i>	
Email	Need to enter manually	
password	Need to enter manually	
Confirm Password	Need to enter manually	
Website	Need to enter manually	
Contact Number	Need to enter manually	

- 3.1.3 Use Cases

USE Case ID:	G.1.1
Release:	1.0
Use Case Title:	
Actors:	Admin
Preconditions:	
Normal Flow:	1. The actor enters User name, email, password ,website ,contact number 2. After entry required field selects the “Save” option. The system validates the information and saves the Company Information.
Alternative Flows:	
Validation:	1. User must enter: a. All field
Post Condition	After saving Merchant Information Admin must fulfill that merchant account

3.1.4 Business Rules: User name will be Unique.

4.1 Merchants

- 4.1.1 Merchant Profile (Merchant Details)

Scope ID	G.1.2.1
General Description	This section will describe the basic information about the Merchant Profile

- 4.1.2 Attribute List

<i>Attribute Name</i>	<i>Description</i>	<i>Effect/Impact</i>
Merchant Name	Need to enter manually	
Contact Number	Automatically	
Organization Name	Need to enter manually	
Organization Address	Need to enter manually	
Organization Phone	Need to enter manually	
Organization Product	Need to enter manually	
Organization Mobile	Need to enter manually	
National ID	Need to enter manually	
Business Type	Need to enter manually	
Passport No	Need to enter manually	
Onetime Charge	Need to enter manually	
Monthly Charge	Need to enter manually	
Security Question	Need to enter manually	
Remarks	Need to enter manually	
Security Question Ans	Need to enter manually	

- 4.1.3 Use Cases

USE Case ID:	G.1.2.1
Release:	1.0
Use Case Title:	Merchant Profile
Actors:	Admin
Preconditions:	
Normal Flow:	<p>The actor enters After entry Organization Product</p> <ol style="list-style-type: none"> 1. Organization Mobile 2. National ID 3. Business Type 4. Passport No 5. Onetime Charge 6. Monthly Charge 7. Security Question 8. Remarks 9. Security Question Answer required field selects the “Save” option. <p>The system validates the information and saves the Merchant Information.</p>
Alternative Flows:	
Validation:	1. User must enter: All the field
Pre-Condition	2. After Create the New Merchant account the go to the Merchant link and hit the profile button
Post Condition	

- 4.1.4 Business Rules

- 1.National ID and passport will be Unique

- 4.1.5 Merchant Bank Detail (Merchant)

Scope ID	1.2.2
General Description	This section will describe the basic information about the Bank.

- 4.1.6 Attribute List

Attribute Name	Description	Effect/Impact
Bank Name	<i>Need to enter manually</i>	Purchase Order
Bank Branch	Need to enter manually	
Bank Account Name	Need to enter manually	
Bank Account No.	Select from the list	

- 4.1.7 Use Cases

USE Case ID:	G1.2.2
Release:	1.0
Use Case Title:	Bank Information
Actors:	Admin
Preconditions:	Create the Merchant Profile
Normal Flow:	The system validates the information and saves the Bank Information.
Alternative Flows:	
Validation:	All field
Post Condition	

- 4.1.8 Business Rules

- Bank Account number should be unique

- 5.1 Merchant Documents Details (Merchant)

Scope ID	1.2.3
General Description	This section will describe the basic information about the Merchant Document.

- 5.1.1 Attribute List

Attribute Name	Description	Effect/Impact
Merchant Logo	Need to enter manually	
Merchant NID	Need to enter manually	
Merchant Profile	Need to enter manually	
Merchant Passport	Need to enter manually	
Merchant Trade License	Need to enter manually	

- 5.1.2 Use Cases

USE Case ID:	G. 1.2.3
Release:	1.0
Use Case Title:	Merchant Documents Details
Actors:	Admin
Preconditions:	
Normal Flow:	<ol style="list-style-type: none"> The actor enters all document information After entry required field selects the “Save” option. The system validates the information and saves the Merchant Documents Details.
Alternative Flows:	
Validation:	All Filed
Post Condition	Merchant NID and Logo should be unique

- 5.1.3 Merchant Password Reset

Scope ID	G. 1.2.4
General Description	This section will describe the basic information about the Change Password.

- 5.1.4 Attribute List

Attribute Name	Description	Effect/Impact
New Password	Need to enter manually	Previous password
Confirm Password	Need to enter manually	

- 5.1.5 Use Cases

USE Case ID:	G. 1.2.4
Release:	1.0
Use Case Title:	Merchant Password Reset
Actors:	Admin
Preconditions:	Set previous password
Normal Flow:	1. After entry required field selects the “Save” option. The system validates the information and saves the Password Information.
Alternative Flows:	
Validation:	All field
Post Condition	

- **5.1.6 Business Rules:** Password will be Unique

6.1 (Setting)

- 6.1.1 Card Detail

Scope ID	G. 1.3.1
General Description	This section will describe the information about Card Details setting

- 6.1.2 Attribute List

Attribute Name	Description	Effect/Impact
Package name	Select from Drop down list	
Override cards	Select card name from dropdown Fill the charge amount, discount, EMI	
Disable cards	Select from drop down list.	
Extra charge	Select from drop down list.	
Emi Extra Charge	Select from drop down list.	
Create Detail	Select from drop down list.	

- 6.1.3 Use Cases

USE Case ID:	G. 1.3.1
Release:	1.0
Use Case Title:	<i>Card Details</i>
Actors:	Admin
Preconditions:	
Normal Flow:	The actor enters Package name, Override cards, Disable cards Extra charge
Alternative Flows:	
Validation:	1. User must enter all field
Post Condition	After saving Information system will be automatically generated Access App Key.

- 6.1.4 Business Rule

7.1 Merchant App Key Details

Scope ID	G. 1.3.2
General Description	This section will describe the information about the new Merchant App Key Details

- 7.1.1 Attribute List

Attribute Name	Description	Effect/Impact
Access Username	Will be auto generated	
Access Password	Will be auto generated	
Access App Key	<i>Will be auto generated</i>	
Merchant Domain	Display from previous data.	
Site Info	Select from list	
Call back URL	Display from previous data.	
Transaction Mode	Select from list	
Merchant ID	<i>Will be auto generated</i>	

- 7.1.2 Use Cases

USE Case ID:	UC-PDMS-G.1.18.1
Release:	1.0
Use Case Title:	Merchant App Key Details
Actors:	Admin
Preconditions:	Save card details
Normal Flow:	After fill, all the mandatory field press create button.
Alternative Flows:	
Validation:	All field
Post Condition	.

- 7.1.3 Merchant Bank Bridge

Scope ID	G. 1.3.3
General Description	This section will describe the information about Merchant Bank Bridge

- 7.1.4 Attribute List

Attribute Name	Description	Effect/Impact
DBBL M ID	Need to enter manually	
DBBL T ID	Need to enter manually	
EBL ID	Need to enter manually	
EBL Pass	Need to enter manually	
DBBL M Name	Need to enter manually	
City Bank ID	Need to enter manually	
Qcash ID	Need to enter manually	
Brac ID	Need to enter manually	
bKash Username	Need to enter manually	
bKash Password	Need to enter manually	
bKash Msisdn	Need to enter manually	
SEBL ID	Need to enter manually	
SEBL Pass	Need to enter manually	

- 7.1.5 Use Cases

USE Case ID:	UC-PDMS-G.1.19.1
Release:	1.0
Use Case Title:	Merchant Bank Bridge
Actors:	Admin
Preconditions:	
Normal Flow:	The actor fills all field according to card setting
Alternative Flows:	
Validation:	According to card name those field will be mandatory
Post Condition	.

- 7.1.6 Business Rules

If card name is DBBL then actor must have fill which are related to DBBL in merchant bank bridge.

- 8.1 Merchant Verify

Scope ID	G. 1.3.4
General Description	This section will describe the information about Merchant Verify

- 8.1.1 Attribute List

Attribute Name	Description	Effect/Impact
Verified Status	Select from the drop-down list	
Banned Status	Select from the drop-down list	

- 8.1.2 Use Cases

USE Case ID:	G. 1.3.4
Release:	1.0
Use Case Title:	Merchant Verify
Actors:	Admin
Preconditions:	Fill all the field of Merchant App Key Details
Normal Flow:	Actor update Verify/ not verify dropdown list
Validation:	
Post Condition	

- 8.1.3 Business Rules

- 9.1 Merchant Filter (Merchant)

Scope ID	G1.4
General Description	This section will describe the information about the Merchant Search

- 9.1.1 Attribute List

Attribute Name	Description	Effect/Impact
Merchant ID	Need to enter manually.	
Username	Need to enter manually.	
Email	Need to enter manually.	
Merchant Name	Need to enter manually.	
Website	Need to enter manually.	
Organization Name	Need to enter manually.	
Signup Time	Need to enter manually.	
Merchant Filter	Need to enter manually.	

- 9.1.2 Use Cases

USE Case ID:	G. 1.4
Release:	1.0
Use Case Title:	Merchant Search
Actors:	Admin
Preconditions:	

- 9.1.3 Business Rules

10.1 Gateway Setting

- 10.1.1 Bank Setting

- 10.1.2 Bank

- 10.1.3 Banks

Scope ID	G. 2.1.1.1
General Description	This section will describe the information bank

- 10.1.4 Attribute List

Attribute Name	Description	Effect/Impact
Bank Name	Display from previous data	
Description	Display from previous data	

- 10.1.5 Use Cases

USE Case ID:	G2.1.1.1
Release:	1.0
Use Case Title:	Banks
Actors:	Admin
Preconditions:	
Normal Flow:	Actor Can only show data
Alternative Flows:	
Validation:	
Post Condition	

- 10.1.6 Business Rules

11.1 Bank create

Scope ID	<i>G. 2.1.1.2</i>
General Description	This section will describe the information about Create bank

- 11.1.1 Attribute List

Attribute Name	Description	Effect/Impact
Bank Name	Enter Manually	
Description	Enter Manually	

- 11.1.2 Use Cases

USE Case ID:	G. 2.1.1.2
Release:	1.0
Use Case Title:	
Actors:	Executive of TSD
Preconditions:	
Normal Flow:	1.The actor enters Bank name and Description
Alternative Flows:	
Validation:	All field
Post Condition	

- 11.1.3 Business Rules

12.1 Card

- 12.1.1 Cards

Scope ID	G. 1.3.3
General Description	This section will describe the information about Merchant Bank Bridge

- 12.1.2 Attribute List

Attribute Name	Description	Effect/Impact
Card name, card Code, Bank Name, Payment Method	Only show from Database	

- 12.1.3 Use Cases

USE Case ID:	UC-PDMS-G. 2.1.2.1
Release:	1.0
Use Case Title:	Card
Actors:	Admin
Preconditions:	After Saving new card show all card in this section.
Normal Flow:	
Alternative Flows:	
Validation:	
Post Condition	

- 12.1.4 Business Rules

13.1 Create Card

Scope ID	G. 2.1.2.2
General Description	This section will describe the information about Create Card

- 13.1.1 Attribute List

Attribute Name	Description	Effect/Impact
Card Name	Manually Entry	
Description	Manually Entry	
Bank Name	Select from dropdown	
Payment Method	Select from dropdown	
Description	Manually Entry	
Card Code	Manually Entry	

- 13.1.2 Use Cases

USE Case ID:	G. 2.1.2.2
Release:	1.0
Use Case Title:	Create Card
Actors:	Admin
Preconditions:	
Normal Flow:	Save all information
Alternative Flows:	
Validation:	All field
Post Condition	

- 13.1.3 Business Rules

14.1 Currency Setting

- 14.1.1 Currencies

Scope ID	G. 2.2.1
General Description	This section will describe the information about Currencies

- 14.1.2 Attribute List

Attribute Name	Description	Effect/Impact
Currency Name, Currency Code, Numeric Code, Country, Conversion Rate, Description, Show	Only show the data	

- 14.1.3 Use Cases

USE Case ID:	UC-PDMS-G.1.26.1
Release:	1.0
Use Case Title:	Currencies
Actors:	Admin
Preconditions:	
Normal Flow:	Only can see all above data
Alternative Flows:	
Validation:	
Post Condition	

- 14.1.4 Business Rules

- 15.1 Create currency

Scope ID	G. 2.2.2
General Description	This section will describe the information about Create currency form Analysis

- 15.1.1 Attribute List

Attribute Name	Description	Effect/Impact
Currency Name	Enter manually	
Currency Code	Enter manually	
Numeric Code	Enter manually	
Conversion Rate,	Enter manually	
Description, Show	Enter manually	
country	Enter manually	

- 15.1.2 Use Cases

USE Case ID:	UC-PDMS-G.1.27.1
Release:	1.0
Use Case Title:	Create currency
Actors:	Admin
Preconditions:	
Normal Flow:	Save all the required field
Alternative Flows:	
Validation:	User must enter: Currency Name, Currency Code, Numeric Code, Country, Conversion Rate, Description, Show
Post Condition	

- 15.1.3 Business Rules

16.1 Package Setting

- 16.1.1 Packages

Scope ID	G. 2.3.1
General Description	This section will describe the information about Packages

- 16.1.2 Attribute List

Attribute Name	Description	
card	Select proposal no from list. List will	
Bank name	Display from previous data	
Code	Display from previous date	
Payment Method	Available from list.	
charge	Need to enter manually.	
Status	Need to enter manually.	
Description	Available from list.	
show	Need to enter manually.	

- 16.1.3 Use Cases

USE Case ID:	UC-PDMS-G.1.28.1
Release:	1.0
Use Case Title:	Packages
Actors:	
Preconditions:	Data come from create packages
Normal Flow:	Fill those field and save
Alternative Flows:	
Validation:	All field
Post Condition	

- 16.1.4 Business Rules

17.1 New Package

Scope ID	G.2.3.2
General Description	This section will describe the information about Create Package

- 17.1.1 Attribute List

Attribute Name	Description	
Package Name	Enter Manually	
Package Price	Enter Manually	
Description	Enter Manually	
Status	Enter Manually	
Card	Select from dropdown list comes from Card	
Charges	Enter Manually	

- 17.1.2 Use Cases

USE Case ID:	G. 2.3.2
Release:	1.0
Use Case Title:	Create Package
Actors:	
Preconditions:	
Normal Flow:	Fill all the information and create
Alternative Flows:	
Validation:	
Post Condition	

- 17.1.3 Business Rules

18.1 Payment (MERCHANT-Account User)

- 18.1.1 Payment

- 18.1.2 Transaction

Scope ID	G. 3.1
General Description	This section will describe the information about Transaction

- 18.1.3 Attribute List

Attribute Name	Description	
CRAFTCODE Trxn ID, Merchant Order ID, Card Number, Min Amount, Max Amount, Transaction Status, Date Range, Bank, Payment Module, Transaction, Transaction ID, Customer Details	Merchant can search though those parameter for result	

- 18.1.4 Use Cases

USE Case ID:	UC-PDMS-G.1.30.1
Release:	1.0
Use Case Title:	Transaction
Actors:	
Preconditions:	
Normal Flow:	Only can search and can send remarks.
Alternative Flows:	
Validation:	
Post Condition	

- 18.1.5 Business Rules

- 19.1 Change Password

Scope ID	G. 3.2
General Description	This section will describe the information about Change Password

- 19.1.1 Attribute List

Attribute Name	Description	
Old password	Enter Manually	
New Password	Enter Manually	
Confirm Password	Enter Manually	

- 19.1.2 Use Cases

USE Case ID:	G-3.2
Release:	1.0
Use Case Title:	Change Password
Actors:	Merchant
Preconditions:	
Normal Flow:	The actor can update his password
Alternative Flows:	
Validation:	1. User must enter: a. old password b. new password
Post Condition	Then Actor can login using his new password

- 19.1.3 Business Rules

20.1 Payment (Admin Side)

- 20.1.1 Transaction

Scope ID	G-4.1
General Description	This section will describe the information about Transaction

- 20.1.2 Attribute List

Attribute Name	Description	
CRAFTCODE Trxn ID, Merchant Order ID, Card Number, Min Amount, Max Amount, Transaction Status, Date Range, Bank, Payment Module, Transaction, Transaction	Search field using those parameters	

- 20.1.3 Use Cases

USE Case ID:	UC-PDMS-G.1.32.1
Release:	1.0
Use Case Title:	Transaction
Actors:	Admin
Preconditions:	
Normal Flow:	Admin can see detail, invoice, comment
Alternative Flows:	
Validation:	
Post Condition	

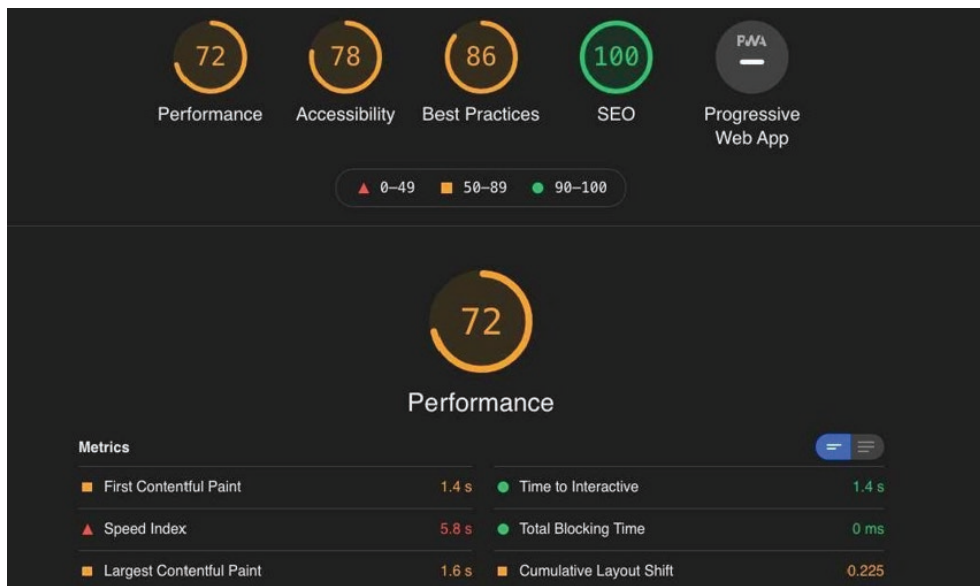
- 20.1.4 Business Rules

Non Functional Requirement Specification (FRS)

Project Name: Payment Gateway powered by Craft Code Ltd.

Company Name: Craft Code Ltd.

- Usability
 - Merchants must change the initially assigned login password immediately after the first successful login. Moreover, the initial should never be reused.
 - Merchants will be redirected to captcha after some unsuccessful login attempts.
 - The payment interface is user-friendly so both the user and merchants can understand.
- Performance and scalability
 - The performance score in Google lighthouse is 72 for admin panel and it takes 1.1 second to return API response in postman.
- Reliability
 - Merchants can check their payment 98% of the time without failure.



- Availability

- Users can make payment using the gateway throughout the week at any time during the day.
- In the case of unplanned system downtime

Sl. No	Issue Name	Time
Category A	Application level bug fixing	1-2 Days
Category B	Procedural level changes	3-7 Days
Category C	Architectural level changes	15 Days

- Maintainability

- If any issue arises in the payment gateway they are fixed as soon as possible and notify the merchants through email and also there is a live support service where merchants can notify their issue to the support system operator and they notify it to the regarding team.

- Recoverability

- If a major incident happens on the payment gateway and, the business must take measures to go back to being fully operational within three days.

- Manageability

- When editing the code for payment gateway, the rest of the site stays up and running. If any major code update is required the site is taken in maintenance mode for several minutes.

- Environmental

- Server Configuration
- The system runs on the Linux operating system. It is hosted on a cpanel server. The server specifications are:

OS	Linux
Server	SOLID BM-1
Processor	1 x Intel Xeon E3-1230 V6
Core	4
RAM	16 GB with Dual Slot
HDD	1TB x 2(+RAID 1) with Dual Slot of SDD Port
Bandwidth	10 MBPS

- Device Configuration
 - The application runs on any Operating system that supports a browser. For Android and iOS there is an individual library. Merchants can use this library for their Android and iOS application.

SOFTWARE QUALITY TEST PLAN

Test Plan: Payment Gateway powered by Craft Code Ltd.

Prepared by: Tasnim Hosen (01.08.2024)

- TABLE OF CONTENTS
 - 1.0 INTRODUCTION
 - 2.0 OBJECTIVES AND TASKS
 - 2.1 Objectives
 - 2.2 Tasks
 - 3.0 SCOPE
 - 4.0 Testing Strategy
 - 4.1 Alpha Testing (Unit Testing)
 - 4.2 System and Integration Testing
 - 4.3 Performance and Stress Testing
 - 4.4 User Acceptance Testing
 - 4.5 Batch Testing
 - 4.6 Automated Regression Testing
 - 4.7 Beta Testing
 - 5.0 Hardware Requirements
 - 6.0 Environment Requirements
 - 6.1 Main Frame
 - 6.2 Workstation
 - 7.0 Test Schedule
 - 8.0 Control Procedures
 - 9.0 Features to Be Tested
 - 10.0 Features Not to Be Tested
 - 11.0 Resources/Roles & Responsibilities
 - 12.0 Schedules
 - 13.0 Significantly Impacted Departments (SIDs)
 - 14.0 Dependencies
 - 15.0 Risks/Assumptions
 - 16.0 Tools
 - 17.0 Approvals

• INTRODUCTION

- The Test Plan has been created to communicate the test approach to team members. It includes the objectives, scope, schedule, risks and approach. This document will clearly identify what the test deliverables will be and what is deemed in and out of scope.

• 2.0 OBJECTIVES AND TASKS

- 2.1 Objectives

- Describe the objectives supported by the Master Test Plan, eg., defining tasks and responsibilities, vehicle for communication, document to be used as a service level agreement, etc.

- 2.2 Tasks

- List all tasks identified by this Test Plan, i.e., testing, post-testing, problem reporting, etc

• 3.0 SCOPE

- The initial phase will include all 'must have' requirements. These and any other requirements that get included must all be tested. At the end of Phase 1, a tester must be able to:
 1. Create a manual test with as many steps as necessary
 2. Save it
 3. Retrieve it and have the ability to view it when running the test
 4. Enter results and appropriate comments
 5. View results
 6. Automation Test
- As the team works with the product they will define the needs for the second phase.

• 4.0 TESTING STRATEGY

The project is using an agile approach, with weekly iterations. At the end of each week the requirements identified for that iteration will be delivered to the team and will be tested. Exploratory testing will play a large part of the testing as the team has never used this type of tool and will be learning as they go. Tests for planned functionality will be created and added to TCT as we get iterations of the product. We have done those testing which are described in below:

• 4.1 Unit Testing

Definition:

Specify the minimum degree of comprehensiveness desired. Identify the techniques which will be used to judge the comprehensiveness of the testing effort (for example, determining which statements have been executed at least once). Specify any additional completion criteria (for example, error frequency). The techniques to be used to trace requirements should be specified.

Participants: Tasnim Hosen & Monjurul Kanon

Methodology: After finishing every module of our system Mr. Nishat will perform unit test. He will be the responsible person for that

• 4.2 System and Integration Testing

Definition:

It is a level of software testing where individual units are combined and tested as a group. The purpose of this level of testing is to expose faults in the interaction between integrated units. Test drivers and test stubs are used to assist in Integration Testing.

Participants: Mr. Kanon, Mr. Nishat & Mr. Nayem

Methodology:

It's a systematic technique for constructing the program structure while conducting tests to uncover errors associated with interfacing.

All modules are integrated in advance, and the entire program is tested as a whole. But during this process, a set of errors is likely to be encountered.

Correction of such errors is difficult because isolation causes is complicated by the vast expansion of the entire program. Once these errors are rectified and corrected, a new one will appear, and the process continues seamlessly in an endless loop. To avoid this situation, another approach is used, Incremental Integration

• 4.3 Performance and Stress Testing

Definition:

Performance Testing is defined as a type of software testing to ensure software applications will perform well under their expected workload.

Features and Functionality supported by a software system is not the only concern. A software application's performance like its response time, reliability, resource usage and scalability do matter. The goal of Performance Testing is not to find bugs but to eliminate performance

Participants: Mr. Tasnim Hosen & Mr. Kanon

Methodology:

Successful performance testing of websites, web apps and APIs requires planning. You may want to jump in, pick a load testing tool and start testing, but let's take some time to establish our methodology first. A software performance testing methodology requires a number of steps. Let's break them down into 3 phases:

- Phase 1- Planning, Test Configuration, and Validation
- Phase 2- Baseline Testing, Scaling Your Tests, and Complex Cases
- Phase 3- Ongoing Performance Testing and Automation

• 4.4 User Acceptance Testing

Definition:

User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications. UAT is one of the final and critical software project procedures that must occur before newly developed software is rolled out to the market. User acceptance testing (UAT), otherwise known as Beta, Application, or End-User Testing, is often considered the last phase in the web development process, the one before final release or installation of the website or software for the client, or final distribution of it.

Participants: Tasnim Hosen & Mr. Kanon

Methodology: After establishing path with client server with we test with client with scenario

• 4.5 Automated Regression Testing

We have used several tools for automation testing. Like

- a. Appium
- b. Selenium
- c. Jmeter
- d. TestNG
- e. ReportNG

• 5.0 HARDWARE REQUIREMENTS

- Computers
- Modems

• 6.0 ENVIRONMENT REQUIREMENTS

- 6.1 Main Frame

- Specify both the necessary and desired properties of the test environment. The specification should contain the physical characteristics of the facilities, including the hardware, the communications and system software, the mode of usage (for example, stand-alone), and any other software or supplies needed to support the test. Also specify the level of security which must be provided for the test facility, system software, and proprietary components such as software, data, and hardware.

• 7.0 TEST SCHEDULE

It depends on client demand and requirements

• 8.0 CONTROL PROCEDURES

Problem Reporting:

- Document the procedures to follow when an incident is encountered during the testing process. If a standard form is going to be used, attach a blank copy as an "Appendix" to the Test Plan..

Change Requests:

- Document the process of modifications to the software. Identify who will sign off on the changes and what would be the criteria for including the changes to the current product. If the changes will affect existing programs, these modules need to be identified.

• 9.0 FEATURES TO BE TESTED

- Identify all software features and combinations of software features that will be tested.

• 10.0 FEATURES NOT TO BE TESTED

- User Web application performance

• 11.0 RESOURCES/ROLES & RESPONSIBILITIES

- Mr. Kanon played QA manager role

• 12.0 SCHEDULES

- Major Deliverables

- Test Plan
- Test Cases
- Test Incident Reports
- Test Summary Reports

• 13.0 SIGNIFICANTLY IMPACTED DEPARTMENTS (SIDs)

Department/Business Area

Bus. Manager

Tester(s)

• 14.0 DEPENDENCIES

- Clint server and other environment

• 15.0 RISKS/ASSUMPTIONS

- The following risks have been identified and the appropriate action identified to mitigate their impact on the project. The impact (or severity) of the risk is based on how the project would be affected if the risk was triggered. The trigger is what milestone or event would cause the risk to become an issue to be dealt with. We have defined those state

#	Risk	Impact	Trigger	Mitigation Plan
1	Scope Creep – as testers become more familiar with the tool, they will want more functionality	High	Delays in implementation on date	Each iteration, functionality will be closely monitored. Priorities will be set and discussed by stake holders. Since the driver is functionality and not time, it may be necessary to push the date out.
2	Changes to the functionality may negate the tests already written and we may lose test cases already written	High - to schedule and quality	Loss of all test cases	Export data prior to any upgrade, massage as necessary and re-import after upgrade.
3	Weekly delivery is not possible because the developer works off site	Medium	Product did not get delivered on schedule	

• 5.0 TEST INSTANCES

- Sometime we had faced some unexpected result like when we integrated it with other server for testing it did not work properly due to mismatch of PHP version. So we reconfigured the server and web application accordingly.

- **APPENDIX A:** Test Report Approval

- The undersigned acknowledge they have reviewed Test Report and agree with the approach it presents. Changes to this Test Report will be coordinated with and approved by the undersigned or their designated representatives

Signature:

Date:

Print Name: Tasnim Hosen

Role: Chief Operating Officer

CraftCode

Wanderstrasse 133
4054 Basel, Switzerland
Phone: +41 798956413

info@craftcode.ch
www.craftcode.ch

CraftCode Dubai

Unit 18, Phase 01, LIU (Light Industrial Unit),
Dubai Silicon Oasis, Dubai, UAE

CraftCode Bangladesh

Suvastu Muskan Tower, Level 7, 56 Gulshan
Avenue, Gulshan 1, Dhaka-1212, Bangladesh
Phone: +8809613443344